FOURTH IN A SERIES OF SUBCOMMITTEE HEARINGS ON SOCIAL SECURITY NUMBER HIGH-RISK ISSUES

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

MARCH 16, 2006

Serial No. 109–58

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

30–704 WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS

BILL THOMAS, California, *Chairman*

E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
PHIL ENGLISH, Pennsylvania
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
MARK FOLEY, Florida
KEVIN BRADY, Texas
THOMAS M. REYNOLDS, New York
PAUL RYAN, Wisconsin
ERIC CANTOR, Virginia
JOHN LINDER, Georgia
BOB BEAUPREZ, Colorado
MELISSA A. HART, Pennsylvania
CHRIS CHOCOLA, Indiana
DEVIN NUNES, California

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
EARL POMEROY, North Dakota
STEPHANIE TUBBS JONES, Ohio
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
RAHM EMANUEL, Illinois

ALLISON H. GILES, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

SUBCOMMITTEE ON SOCIAL SECURITY

JIM MCCRERY, Louisiana, *Chairman*

E. CLAY SHAW JR., Florida
SAM JOHNSON, Texas
J.D. HAYWORTH, Arizona
KENNY C. HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin

SANDER M. LEVIN, Michigan
EARL POMEROY, North Dakota
XAVIER BECERRA, California
STEPHANIE TUBBS JONES, Ohio
RICHARD E. NEAL, Massachusetts

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

FOURTH IN A SERIES OF SUBCOMMITTEE HEARINGS ON SOCIAL SECURITY NUMBER HIGH-RISK ISSUES

THURSDAY, MARCH 16, 2006

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:03 a.m., in room B–318, Rayburn House Office Building, Hon. Jim McCrery (Chairman of the Subcommittee) presiding.

[The advisory announcing the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
March 8, 2006
SS–13

CONTACT: (202) 225–9263

McCrery Announces Fourth in a Series of Subcommittee Hearings on Social Security Number High-Risk Issues

Congressman Jim McCrery, (R–LA), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold the fourth in a series of Subcommittee hearings on Social Security number (SSN) high-risk issues. The hearing will examine expanding uses of the SSN card and measures to prevent SSN card fraud. **The hearing will take place on Thursday, March 16, 2006, in room B–318 Rayburn House Office Building, beginning at 10:00 a.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

The SSN was created in 1936 to record earnings and benefits for the Social Security program. The sole purpose of the SSN card was to show that an SSN had been issued to the named individual. Originally, the SSN card had no security features other than the individual's signature.

Within a decade, the SSN's use grew beyond its original narrow purpose, and has continued to expand. According to the Social Security Administration (SSA), the SSN is now the single most widely-used record identifier for both the government and the private sectors.

As with the SSN, the SSN card's uses also have expanded over the decades. Currently, one of its most important roles is in work authorization. The U.S. Department of Homeland Security requires employers to document the identity and employment eligibility of their new hires. For U.S. citizens and some non-citizens, employers may accept the SSN card as proof of a person's eligibility to work in the United States.

As the uses of the SSN and the SSN card have increased, security features have been added to the SSN card to prevent its fraudulent duplication or alteration. For example, legislation enacted in the early 1980s required specific changes to the SSN card, and the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108–458) requires that standards be established and implemented to safeguard SSN cards from counterfeiting, tampering, alteration, and theft. However, the SSA does not replace all existing SSN cards when a new SSN card design is adopted, due to workload concerns and the potential burden on the public. As a result, since 1936, the SSA has issued more than 433 million SSNs, with about 50 different versions of the SSN card—all of which are still valid.

Despite its adoption for other purposes, the SSN card by itself is not a personal identity document. The SSN card does not contain information that would confirm that the person presenting the card is actually the person whose name and SSN appear on the card. Several bills introduced in the 109th Congress would mandate significant changes to the card for that purpose. For example, one proposal would enhance the security features in the SSN card as part of a package of changes to the

process of confirming the identity and work eligibility of new hires. However, ideas such as adding photographs, machine-readable electronic strips, and other features to SSN cards have raised concerns about the future purpose of the card. Some have expressed concerns that SSN card may evolve into a form of national identification.

In announcing the hearing, Chairman McCrery stated, "Because of the expanding use of SSNs and SSN cards, they are often transformed into tools to gain illegal employment and perpetrate identity theft and other crimes. We need a thorough examination of the appropriateness of using SSNs in certain roles. It is equally important for us to examine the potential impact on individual's security and privacy that could result from changes to the design of the SSN card."

FOCUS OF THE HEARING:

The Subcommittee will examine the history of SSNs and SSN card use, the role of the SSN card in work authorization, measures to prevent SSN card fraud, and the potential effects of transforming the SSN card into an identification document.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov*, select "*109th Congress*" from the menu entitled, "*Hearing Archives*" (*http://waysandmeans.house.gov/Hearings.asp?congress=17*). Select the hearing for which you would like to submit, and click on the link entitled, "*Click here to provide a submission for the record*." Once you have followed the online instructions, completing all informational forms and clicking "submit" on the final page, an email will be sent to the address which you supply confirming your interest in providing a submission for the record. You ***MUST REPLY*** to the email and ***ATTACH*** your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, by close of business Thursday, March 30, 2006. **Finally**, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225–1721.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word or WordPerfect format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. All submissions must include a list of all clients, persons, and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone and fax numbers of each witness.

Note: All Committee advisories and news releases are available on the World Wide Web at *http://waysandmeans.house.gov*.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Chairman MCCRERY. The hearing will come to order. Good morning, and welcome to our fourth in a series of hearings on high risk issues related to Social Security numbers (SSNs). Today, we will examine the expanding uses of the SSN and options to prevent fraud involving SSN cards, and in the interests of time, because we are going to have votes coming up pretty soon, I am going to submit the rest of my opening statement in writing for the record, and I would yield to my colleague, the Ranking Member, Mr. Levin.

[The prepared statement of Chairman McCrery follows:]

Opening Statement of The Honorable Jim McCrery, Chairman, and a Representative in Congress from the State of Louisiana

Good morning and welcome to our fourth in a series of hearings on high-risk issues related to Social Security numbers, or SSNs. Today, we'll examine the expanding uses of the SSN and options to prevent fraud involving SSN cards.

Much of our discussion at this hearing will focus on the use of the SSN and SSN card in employment. Current law requires employers to verify the identity and employment eligibility of new hires. Employers may accept an SSN card as one of several documents that a person may present as proof of employment eligibility, if the card does not bear either of two legends: "Not Valid for Employment" or "Valid for Work Only with DHS Authorization."

After examining a new hire's documents; the employer must accept them, if the documents reasonably appear to be genuine and belong to the worker. If an employee uses an SSN card to prove work authorization, he or she must provide another document to prove his or her identity, such as a driver's license.

To simplify the process for employers and prevent unauthorized work, some legislators have proposed making the SSN card the single, counterfeit and tamper-resistant document employers would be required to see, replacing all the others. The SSN card would be modified to contain proof of identity. Employers would use it to access a government database to verify employment eligibility.

Such a change would greatly expand the role of the SSN card in work authorization, and it raises a number of essential questions that I hope we will address today.

First, how confident can we be that a particular SSN was issued based on accurate information? The answer, as we have learned from previous hearings, depends on when the SSN card was issued. It wasn't until 1978 that all SSN applicants were required to provide proof of their identity, age, and citizen or non-citizen status. Before 2002, the Social Security Administration did not consistently verify birth certificates or immigration documents with the issuing agency.

Adding new security features to the SSN card today will not assure the accuracy of the data originally used to issue an SSN. To raise the level of accuracy, all SSN cardholders in the workforce would have to apply for new cards and provide full documentation of their identity, citizen or non-citizen status, and age. What would this cost? What impact would this have on the Social Security Administration?

Second, what are the options for designing a counterfeit and tamper-resistant SSN card? As required by the Intelligence Reform and Terrorism Prevention Act of 2004, the Social Security Administration is working with the Department of Homeland Security to improve the security of SSNs and SSN cards and implement such improvements by June 2006. It is important to establish the range of options for a counterfeit and tamper-resistant card, the costs of the options, whether the options will work, as well as non-SSN card options to verify identity and work authorization.

Third, what are the ramifications of transforming the SSN card into an identity card? Currently, the SSN card serves only to show that an SSN was assigned to the individual named on the card. It does not contain features to prove that the cardholder is the individual named on the card.

Changing the SSN card into an ID could encourage its use for other purposes, given the widespread use of the SSN itself in many personal and financial transactions. Adding identification features to the SSN card could duplicate efforts already underway to provide secure identity documentation—such as improved driver's licenses and State-issued ID cards called for under the REAL ID Act.

Finally, we must be mindful to examine these issues in a greater context. For example, if employers are ultimately required to verify SSNs and employment eligibility through a government database (as required under some proposals), then employers may only need proof of the worker's identity. The database could confirm

the person's SSN and employment eligibility without the need for an enhanced SSN card.

I look forward to hearing the testimony and recommendations of our witnesses and welcome the views of my colleagues on these complex issues. I believe that it is our responsibility as legislators to work for a balanced, thoughtful approach—one that will deter unauthorized employment without placing undue burdens on businesses, while protecting the privacy of our fellow Americans.

Mr. LEVIN. I will do likewise, so we can hear your testimony and have an hour to think about it.

[Laughter.]

Mr. LEVIN. Thank you.

[The prepared statement of Mr. Levin follows:]

Opening Statement of The Honorable Sander M. Levin, a Representative in Congress from the State of Michigan

Today our Subcommittee has the opportunity to examine two issues—our ongoing, non-controversial effort to ensure that Social Security cards are not counterfeited, and the more controversial debate about whether it is appropriate to make the Social Security card into a national identification card.

These are issues squarely within the jurisdiction of the Ways & Means Committee. I am pleased that the Chairman has provided this opportunity for us to discuss them and to learn more about the proposals and the issues from our colleagues and a panel of experts.

As the Committee of jurisdiction, it is also our responsibility to oversee the efforts already underway. As required by the Intelligence Reform and Terrorism Prevention Act of 2004, the Social Security Administration and the Department of Homeland Security are currently identifying options for making Social Security cards more secure, with the goal of implementing improvements by this June. Each option imposes certain costs, both in dollars and in loss of personal privacy, so it is important for our Committee to weigh the costs and benefits and to keep in close touch with the agencies involved.

I look forward to a frank and thoughtful discussion of these complex issues.

Chairman MCCRERY. Thank you, Mr. Levin. We are also going to reverse the order of the panels this morning so that we can allow these gentlemen to get their testimony in and perhaps go through a few questions before votes are called, and then, the first panel, which consists of two of our colleagues, we will retrieve as we can and then finish the hearing, but that way, we will not have you all sitting around on your thumbs all morning.

With that, I would introduce our first panel this morning: the Honorable Patrick O'Carroll, Inspector General, Social Security Administration (SSA), and he is accompanied this morning by Richard Outland, Branch Chief, Questioned Document Branch, Forensic Services Division, U.S. Secret Service; and Mr. Frederick G. Streckewald, Assistant Deputy Commissioner, Disability Income Security Programs, the SSA; welcome back, both of you gentlemen; Stephen Kent, Chairman, Committee on Authentication Technologies and their Privacy Implications, National Research Council, the National Academies; and Marc Rotenberg, President, Electronic Privacy Information Center. Welcome, all of you gentlemen, and we will begin with Mr. O'Carroll.

STATEMENT OF THE HONORABLE PATRICK O'CARROLL, INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, ACCOMPANIED BY RICHARD OUTLAND, BRANCH CHIEF, QUESTIONED DOCUMENT BRANCH, FORENSIC SERVICES DIVISION, U.S. SECRET SERVICE

Mr. O'CARROLL. Good morning, Chairman McCrery, Congressman Levin. Thank you for inviting me to be here today. I would like to focus on our investigative efforts with respect to SSN misuse.

With me today is Mr. Richard Outland, Assistant Chief, U.S. Secret Service, Forensic Services Division. Based on a longstanding interagency agreement, when our agents come across suspected counterfeited Social Security cards, they are referred to the Secret Service for further forensic examination. Mr. Outland is here today to answer any technical questions.

No matter how carefully we protect the SSN, there will be those who find a way to turn the number to nefarious purposes, and when they do, our special agents will be there. Our statutory mission is to protect the SSA's programs and operations from fraud, and abuse. At the core of that mission is the protection of the Social Security Trust Funds that provide benefits to millions of Americans every month.

To that end, 79 percent of our cases we investigated last year were for program fraud. Still, we are ever mindful of our obligation to protect the SSN from misuse. In fact, 16 percent of our investigations involved SSN misuse.

To maximize our resources, we focus our overall SSN misuse energies in cooperative efforts with other Federal, State, and local task forces. At last count, we were involved in almost 200 task forces and work groups across the country. For example, our agents on the Central Florida Identity Theft Task Force concluded a case last year in which they apprehended 15 members of an identity theft ring. They would obtain lists of individuals with good credit histories and use the personal information of those individuals to defraud a variety of commercial entities in the Orlando area. Twelve of the 15 individuals arrested were sentenced to prison, and all were ordered to repay more than $2 million to the victims.

Our own internal caseload is no less daunting, and our solo work is equally impressive. We see allegations of SSN misuse in myriad forms every day. One such allegation from a SSA district office concerned a woman who was receiving disability benefits under two separate SSNs and insisted that she was one half of a set of identical twins. Our investigators asked her to provide a copy of her birth certificate, while unbeknownst to her, we were obtaining one directly from the State Bureau of Vital Statistics. The one we obtained showed a single birth, and the altered one she produced had the same control number and signatures but showed a twin birth.

Before we confronted her with the fact that we had uncovered her forgery, she had asked her Congressman to intervene on her behalf and demanded that her nonexistent twin's benefits be reinstated. We were only too happy to share the forged birth certificate with the Congressman.

We see SSN misuse cases like this every day. What we see less frequently, however, are cases involving counterfeit Social Security

cards. While we take such cases very seriously and have recently disrupted several counterfeit identity operations, the reality is that the Social Security card serves as little more than a hard copy record of a number that we all memorize at an early age.

While the SSN itself is necessary to obtain employment, to obtain a loan, and for countless other purposes, we rarely, if ever, are asked to show anyone our Social Security cards. The card was designed for a single purpose: to provide the holder with a number used to track earnings and pay benefits.

While the uses of the number have expanded significantly over the decades, the uses of the card have remained more or less the same. There is no question that periodic security improvements to the card are necessary to stay one step ahead of tech savvy counterfeiters. As long as the use of the card remains as limited as it has been, it is difficult to justify the expense that would be incurred in creating a "counterfeit card."

Of course, if Congress decides to expand the uses of the Social Security card, then, those expenses might become necessary. If this is Congress' ultimate decision, we will do everything possible to work with you and the SSA to make the card as counterfeit-proof as possible. Until then, we will continue our audit and investigative efforts to combat SSN misuse and provide the SSA and Congress with timely and accurate information.

Thank you, and if you have any questions, I will be happy to answer them.

[The prepared statement of Mr. O'Carroll follows:]

Statement of The Honorable Patrick P. O'Carroll, Inspector General, Social Security Administration; accompanied by Richard L. Outland, Assistant Branch Chief—Questioned Document Branch, Forensic Services Division, U.S. Secret Service

Good morning, Chairman McCrery, Congressman Levin, and Members of the Subcommittee. This is our fourth hearing in this series on high-risk Social Security number (SSN) issues, and I applaud your efforts and dedication in giving these issues the attention they deserve. The SSN is a key to American life in many ways, and as we have seen throughout this series of hearings, its misuse has repercussions that cause a ripple effect across the American landscape.

Much of my testimony in the first three hearings has centered on largely administrative issues. At the first hearing, we discussed enumeration, the process by which the Social Security Administration (SSA) issues SSNs; at the second hearing, we discussed SSN misuse in the context of misreported wages, particularly by foreign-born workers without authorization to work in the United States; and, at the third hearing earlier this month, we discussed enumeration of foreign-born individuals and the payment of benefits to those born or residing abroad.

Today, I would like to discuss our investigative efforts to combat SSN misuse in all forms. Our Office of Investigations (OI) is dedicated to preventing and detecting fraud against SSA's programs and operations, and SSN misuse is an important facet of that overall investigative effort. Obviously, with finite resources, and with many areas of responsibility, including program fraud, employee fraud, contract fraud, and others, we are mindful that our primary responsibility is to protect the Trust Funds that provide benefits to millions of Americans every month. At the same time, our responsibility to protect the integrity of the SSN cannot be overstated. We strive continuously to strike an appropriate balance.

To give you some sense of how we strike that balance, consider that in Fiscal Year (FY) 2005, the Office of the Inspector General (OIG) received about 85,000 allegations of fraud, 84 percent of which involved fraud against a Social Security program, such as disability insurance benefits. Approximately 13 percent—almost 11,000 allegations—involved SSN misuse. It is important to understand that these SSN misuse allegations are limited to incidents of SSN misuse involving a Social Security program or otherwise directly related to the administration of the Social Security Act.

Allegations of pure identity theft, financial fraud, and other non-SSA-related crimes are referred to appropriate sources, and are not included in this total.

Looking at actual investigations conducted during FY 2005, OI opened approximately 9,500 cases, of which 79 percent involved crimes against Social Security programs, while just over 16 percent involved SSN misuse. Thus, while we actually investigate a higher proportion of allegations in the SSN misuse category than in the program fraud category, we still invest more than four times more resources in program fraud than in SSN misuse. The results of an audit we will issue shortly, in which we provide an estimate of the rate of overpayments in Social Security's disability programs, underscores the importance of our emphasis on program fraud. Our statutory mission is to protect SSA programs and operations, and to the extent that an allegation of SSN misuse does not touch on those programs, our resources do not generally allow us to pursue it.

We do, however, play a role in the overall government effort to protect against SSN misuse in a multijurisdictional context. Our affirmative and aggressive approach to SSN misuse of this type is designed to maximize our resources through the effective use of task forces, workgroups, and other cooperative efforts.

At this time, our investigators across the country are members of almost 200 task forces and workgroups in all ten of our field divisions. These groups, comprised of Federal, State, and local law enforcement agencies, pool resources and, when permitted, share information to accomplish more than each member could ever accomplish on its own. The groups range from Joint Terrorism Task Forces run by United States Attorneys, to white collar crime groups, to financial fraud workgroups.

The work done by these groups is astounding. For example, our agents on the Central Florida Identity Theft task force, a group comprised of ten law enforcement agencies, concluded a case last year in which they apprehended fifteen members of an identity fraud ring who would obtain lists of individuals with good credit histories, and use the personal information of those individuals to defraud a variety of commercial entities in the Orlando area. Twelve of the fifteen individuals arrested were sentenced to prison terms, and the total restitution ordered to victims exceeded $2 million.

In another case, our New York Field Division, working on a task force with other agencies including the U.S. Secret Service, investigated the hijacking of a deceased Social Security beneficiary's bank account. The complex investigation revealed that the subjects not only continued to receive the deceased woman's benefits—totaling some $80,000—but also used her bank account to launder counterfeit checks created with the help of a corrupt bank employee. They then went on to steal other SSNs and identities and open additional accounts, which they would use both to create additional fraudulent checks and to launder them. In all, they cashed about $300,000 in bad checks and opened credit card accounts from which they stole another $100,000.

Since cases like this represent an opportunity to achieve a significant return with only minimal investment of resources—our agent in this ten-agency task force still maintains a "normal" caseload—we can afford to contribute substantially to the overall effort to stop SSNs being used as instruments of a crime. If each of the 200 task forces in which we participate makes only a few cases like this each year, we are able to have a far greater effect than we could ever have working alone.

However, our day-to-day program-related SSN misuse caseload is no less daunting, and our solo work is equally impressive. We see allegations of SSN misuse in its myriad forms come in every day by phone, fax, e-mail, and in electronic referrals from SSA employees. One such referral from an SSA District Office concerned a woman who was confronted by SSA with the fact that she appeared to be receiving disability benefits under two separate SSNs. Each set of benefits was going to the same name, the same address, and for the same disability, but under two different SSNs. The woman informed SSA, and subsequently our investigators, that she had a twin sister. Despite the fact that both sets of benefits were going to the same address, the woman alleged that she and her identical twin were estranged and did not speak.

Our investigators obtained a copy of the woman's birth certificate from the state vital records office. It showed that hers had been a single birth, not a twin birth. Additional investigation uncovered no other evidence that a twin had ever existed. Our investigators asked the woman to provide a copy of her birth certificate, and she eventually provided the same document we had obtained from the state without her knowledge. It had the same control number and the same signatures, but the altered copy she provided showed a twin birth. We recontacted the vital statistics office and confirmed that no official change had been made since we'd obtained our copy. The woman, unaware that we had her original birth certificate, continued to demand that her duplicate benefits be reinstated, even going so far as to write to

her Congressman to demand that he intercede on her behalf. We showed the Congressman the two versions of the birth certificate, and that ended the woman's ill-conceived mission.

In another case, our investigation revealed that a woman had been working full-time since 1978 under one SSN and receiving Title XVI disability payments since 1973 under a second SSN. From 1978 until 2001, she worked full-time for various healthcare agencies while certifying each year to SSA that she was not working. In 2001, the woman applied for Title II disability benefits under the first SSN, based on her extensive work history. A Title XVI claims representative recognized the woman during her appointment to apply for Title II benefits, and referred the case to OIG. She later admitted to OIG agents that she had been working for 23 years while receiving Title XVI payments. She eventually pled guilty to theft of government funds and making false statements, and was sentenced in May 2005 to 6 months' incarceration in federal prison, 6 months' home detention with an electronic monitoring device, and 5 years' probation, and was ordered to pay full restitution of $166,767.

While SSN misuse cases like these are made by our investigators every day, we encounter cases involving counterfeit Social Security cards much less frequently. The practical reality is that most of us were issued our Social Security cards not long after we were born, and we long ago committed our SSNs to memory. But the cards themselves were probably placed in a drawer or box many years ago, and have rarely been seen or used since. Almost every entity imaginable, from government, to medical facilities and insurance carriers, to creditors, to employers and beyond may and often do ask for SSNs; but rarely, if ever, do they ask to see the card itself.

Our work reviewing SSA's automated employee verification services, such as the Social Security Number Verification Service (SSNVS), further underscores this reality. Employers seeking to confirm the SSN of a current or prospective employee need only take advantage of this service to go online and match the employee's name, SSN, date of birth, and gender against SSA's records—all without ever laying eyes on an actual Social Security card. Of course, for verification services such as SSNVS to be truly effective, we must be confident that the information in SSA's databases is as accurate as possible, and our prior audit work has revealed that this may not always be the case. Nevertheless, SSNVS and other verification services even further minimize the need to carry or present the card. Indeed, today, the card is little more than a "hard copy" of a number that is already contained in various databases throughout society and government. This is consistent with the purpose for which the card was created 70 years ago, and while there should always be security enhancements made to stay one step ahead of tech-savvy counterfeiters, it would be hard to justify the expense involved in replacing all Social Security cards with "hard" cards as long as their utility remains as limited as it is.

From time to time, there is talk of expanding the card's use beyond its current functions, and obviously, this issue is one for Congress to debate. If a decision is made to transform the Social Security card into something more than it is, significant improvements may then have to made in the document. Moreover, it could create a significant new workload for SSA—one that might fall outside of the Agency's current and historical function, or even further heighten the tension between service and integrity.

Whatever Congress may determine is an appropriate role for the Social Security card to play, our office is happy to provide whatever audit and investigative work might prove helpful. In the interim, we will continue our tireless efforts to prevent and detect misuse of the Social Security number as well as the Social Security card itself.

Chairman MCCRERY. Thank you, Mr. O'Carroll. Mr. Streckewald.

STATEMENT OF FREDERICK G. STRECKEWALD, ASSISTANT DEPUTY COMMISSIONER FOR PROGRAM POLICY, OFFICE OF DISABILITY AND INCOME SECURITY PROGRAMS, SOCIAL SECURITY ADMINISTRATION

Mr. STRECKEWALD. Thank you, Mr. Chairman, Mr. Levin. Thank you for inviting me here today to discuss the SSA's enumeration process. This is the process used to assign a SSN to an

individual. This series of Subcommittee hearings highlights the importance of this core agency function. I will summarize my written statement and will ask that it be included for the record.

The Social Security card was never intended and does not serve as a personal identification document; that is, the card does not establish that the person presenting it is actually the person whose name and SSN appear on the card. Although the SSA has made many changes to make it counterfeit-resistant, the card does not contain information that would allow the card to be used as proof of identity.

Beginning in 1983, the Social Security Act (P.L. 74–271) required that SSN cards be made of banknote paper and to the maximum extent practicable, be a card that cannot be counterfeited. The SSA worked with the Bureau of Engraving and Printing, the Secret Service, and the Federal Bureau of Investigation to design a card that met these requirements. All Social Security cards issued since October 1983 incorporate a number of security features intended to make the card counterfeit-resistant and tamper-proof.

Some of these features include but are not limited to a tamper-proof, marbleized background, intaglio printing in some areas of the printing in the card, and colored planchets, which are small disks, randomly displayed on the card. Obviously, some security features have not been made public; other features—some features have been made public; others have not in order to protect the security of the card.

As required by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (P.L. 108–458), the SSA, in consultation with the U.S. Department of Homeland Security (DHS), formed a task force to establish requirements that will further improve the security of SSNs and cards. The task force is considering a wide range of security features that would strengthen the Social Security card, and we will develop a plan for implementing the task force recommendations.

Last year, we estimated that a card with enhanced security features, such as biometric identifiers, would cost approximately $25 per card, not including the startup investments associated with the purchase of equipment needed to produce and issue this type of card. While any estimate would ultimately depend upon the details of the proposal, last year's estimate of replacing cards for 240 million cardholders nationwide was approximately $9.5 billion.

Currently, however, we know the cost of issuing an SSN card has increased by approximately $3 due to new requirements for additional verification of evidence. So, we anticipate an increase in the total cost estimate when we update our figures to reflect current dollar costs.

It is important to note that just as a SSN card does establish identity, neither does it always reflect the individual's current authorization status. The SSN card only reflects an individual's work authorization status at the time the card was issued. It is a snapshot in time. An individual's work authorization status may change over the years, and DHS has sole jurisdiction over the work authorization for noncitizens.

Over the years, the SSA has made continued enhancements to the Social Security card. Due to the substantial cost of replacing all

cards in use, older versions of the card remain valid. Thus, there are about 50 different variations of the SSN card in use that have been issued since 1936.

In addition to the changes the SSA made after September 11, which I have outlined in previous hearings before the Subcommittee, the IRTPA contains several additional provisions to strengthen the integrity of our enumeration process. Two key provisions include the implementation of limits on the number of replacement cards an individual can receive, three per year and ten per lifetime.

With limited exceptions and the addition of death and fraud indicators to SSN verification routines for employers, State agencies issuing drivers' licenses and identity cards and other verification routines as determined to be appropriate. The SSA implemented the restrictions on replacement SSN cards effective December 17, 2005, as required by the IRTPA law. In addition, we place death indicators on our SSN verification services with the Department of Motor Vehicles and employers on March 6, 2006, also ahead of time, required by the law. We continue to work to ensure that fraud indicators will be addressed, added to the SSN verification by December 2007, which is the legislatively mandated date.

In conclusion, we must remember that with all of the improvements in the assignment of SSNs, the Social Security card is still just a record of the SSN assigned to the individual, and it is not an identity document. I look forward to working with you to continue to improve the SSA's processes, and I will be happy to answer any questions you might have.

[The prepared statement of Mr. Streckewald follows:]

Statement of Frederick G. Streckewald, Assistant Deputy Commissioner, Disability and Income Security Programs, Social Security Administration

Mr. Chairman and Members of the Committee:

Thank you for inviting me today to discuss the Social Security Administration's (SSA's) enumeration process. This is the process used to assign a Social Security Number (SSN) to an individual. This series of hearings the Subcommittee is holding have served to highlight the importance of this core agency function. As stewards of the Social Security program, one of our strategic objectives is to strengthen the integrity of the enumeration process. We recognize that protection of the SSN is one of the top issues facing SSA management, and I am pleased to have the opportunity to discuss SSA's enumeration process.

History of the Social Security Number and Card

The Social Security Number is a nine-digit number, used to identify the record of earnings an individual has in employment or self-employment. A numbering system that is based on digits allows for the orderly assignment of numbers and for the potential assignment of as many as 900 million unique SSNs excluding the 900 series reserved for the use of the Internal Revenue Service (IRS). SSA has assigned over 436 million SSNs since 1936.

At the time the Social Security card was developed, its only purpose was to provide a record of the number that had been assigned to the individual so that employers could accurately report the earnings of people who worked in jobs covered under the new Social Security program. This is still the primary purpose for which SSA assigns a number and issues a card.

The card was never intended and does not serve as a personal identification document—that is, the card does not establish that the person presenting it is actually the person whose name and SSN appear on the card. Although SSA has made many changes to make it counterfeit resistant, the card does not contain information that would allow the card to be used as proof of identity.

Use of the SSN Expands Over Time

The purpose of the SSN and card was narrowly drawn at the beginning of the program. However, the use of the SSN as a convenient means of identifying records in large systems of records increased over the years. In 1943, Executive Order 9397 required Federal agencies to use the SSN in any new record system maintained on individuals. Using the SSN as an identifier in federal record systems proved to be an early reflection of what has become an enduring trend expanding the uses of the SSN.

The simplicity and efficiency of using a seemingly unique number that most people already possessed encouraged widespread use of the SSN by both government agencies and private enterprises. As record-keeping and business systems moved to automated data processing, the characteristics of the SSN made it a popular choice for record identification. In 1961, the Federal Civil Service Commission established a numerical identification system for all Federal employees using the SSN as the identification number. The next year, the IRS decided to begin using the SSN as its taxpayer identification number (TIN) for individuals. In 1967, the Defense Department adopted the SSN as the service number for military personnel. At the same time, use of the SSN for computer and other accounting systems spread throughout State and local governments and to the private sector, especially to banks, credit bureaus, hospitals, and educational institutions. There were no legislative restrictions on the use of the SSN at that time.

Statutory Provision Relating to the Public Sector

The first explicit statutory authority to issue SSNs was enacted in 1972. Prior to that time, SSNs were issued pursuant to administrative procedures that the Agency had established. Subsequent Congresses have enacted legislation requiring individuals to have an SSN in order to receive Supplemental Security Income (SSI), Temporary Assistance for Needy Families (TANF), Medicaid, and food stamps. Additional legislation authorized States to use the SSN in the administration of tax, general public assistance, driver's license, and motor vehicle registration laws.

Partly in response to concerns about the proliferation of the use of the SSN, Congress enacted the Privacy Act of 1974. It provided that, except when disclosure is required by Federal statute or by state or local statute or regulation adopted prior to January 1975, no Federal, State, or local government could withhold a right, privilege or benefit from a person simply because the person refused to furnish his or her SSN.

In the 1980s and 1990s, new legislation authorized additional governmental uses of the SSN, including income and eligibility verification, military draft registration, and for operators of stores that redeem food stamps. Legislation was also enacted that required taxpayers to provide the SSNs of dependents on tax returns.

A further expansion of the government's use of the SSN was included in welfare reform legislation enacted in 1996. In order to improve child support enforcement, Congress required the SSN to be recorded in a broad array of records, including applications for professional licenses and marriage licenses, and placed in the record of divorce decrees, support orders, and paternity determinations.

Use of the SSN by the Private Sector

Generally, there are no restrictions in Federal law on the use of the SSN by the private sector. Businesses may ask for a customer's SSN for such things as renting a video, applying for credit cards, obtaining medical services, and applying for public utilities. Customers may refuse to provide their number; however, a business may, in turn, decline to furnish the product or service.

Continuing advances in computer technology, the ready availability of computerized data, and rapidly increasing use of the internet have encouraged the growth of information brokers who amass and sell large volumes of personal information, including SSNs collected by businesses. When possible, information brokers store and retrieve information about an individual by that individual's SSN because the SSN provides an easy method of maintaining computerized records and can be used to compare those records with other business systems which may also use the SSN as a file identifier.

Contemporary Challenges Regarding the Use of the SSN

The use of the SSN has become widespread in our society. The cumulative effect has been that the SSN has become the most widely used identifier by both government and the private sector in establishing and maintaining information about a given individual in various public as well as private record systems. An unintended consequence is that the SSN has also become a tool used by those intent on stealing another person's identity or creating a false identity. We are very concerned about

the misuse of the SSN, and we work closely with SSA's Inspector General, the Federal Trade Commission and the Department of Justice to help deter identity theft and assist in the apprehension and conviction of those who engage in this crime.

Assignment of the SSN

The Number

Prior to 1972, SSNs and cards were issued in our local field offices. Since 1972, SSNs have been issued centrally.

Generally, to obtain an SSN, individuals must apply for an SSN by filing a signed Form SS–5 "Application for a Social Security Card" and by submitting the required evidence. Currently, all applicants for an original number and card must submit evidence of age, identity, and United States citizenship or alien status to a Social Security field office (FO). FO personnel assist with the completion of the SS–5 application. Applicants for replacement Social Security cards must submit evidence of identity, and foreign born applicants must also provide evidence of their immigration status. The SS–5 application includes information about the applicant's name, mailing address, citizenship, sex, race/ethnic description (optional), date and place of birth, mother's maiden name and SSN, and father's name and SSN. However, a parent's SSN is only required for applicants for an original SSN who are under age 18.

While the information required on the SS–5 application has remained essentially the same over the years, the law and enumeration process have changed to ensure that SSA assigns SSNs only to eligible individuals. To strengthen the process, SSA has instituted additional safeguards to prevent a person from fraudulently obtaining an SSN. For example:

- SSA verifies immigration status with DHS before assigning an SSN to a non-citizen.
- SSA requires a mandatory in-office interview with all applicants age 12 or older since the majority of individuals born in the U.S. have been assigned an SSN by the time they reached age 12.
- As a result of Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law (P.L.)108–458, SSA implemented policy changes effective December 17, 2005 that restrict the issuance of replacement SSN cards to no more than three per year and no more than ten per lifetime; establish minimum verification standards for documents submitted in support of an application for an SSN; and require independent verification of birth records of individuals of all ages applying for an original SSN card.
- Effective November 2005, we added systems edits to our Enumeration at Birth (EAB) program so that children who have not yet been given a first name in the hospital are not assigned a Social Security Number until the parent submits documentation of the child's name. SSA has also implemented additional safeguards designed to prevent the assignment of multiple SSNs to the same child.

I would also like to highlight some earlier changes that SSA implemented over the years to strengthen the enumeration process.

At the inception of the program, all SSNs were assigned and cards issued based solely on information provided by the applicant. Evidence of identity was not required. Over time, as the use of the number was expanded for other purposes, SSA recognized that changes were necessary to protect the integrity of the card and enumeration process. Beginning in November 1971, persons age 55 and over applying for an SSN for the first time were required to submit evidence of identity. As of April 1974, non-citizens were required to submit documentary evidence of age, identity and immigration status. This made it more difficult to obtain a card on the basis of a false identity. SSA was also concerned that individuals who had been assigned SSNs for purposes other than work might use the card to obtain unauthorized employment. Therefore, in July 1974, we began to annotate our records to reflect the fact that a non-citizen had been issued an SSN for nonwork purposes. Several years later, the integrity of the SSN was further improved. In May 1978, we began requiring all SSN applicants to provide evidence of age, identity and United States citizenship or non-citizen status.

Enumeration at Birth Process (EAB)

Because of increased demand for SSNs for children at earlier ages due to tax and banking requirements, SSA developed the EAB process in 1987. SSA recognized that all the information needed to process an SSN application for a newborn was gathered by hospital employees at the child's birth and verified with the respective bureaus of vital statistics. Nearly three-quarters of all requests for an original SSN are now completed through this process.

This program is available in the fifty states, the District of Columbia, and Puerto Rico, and allows parents to indicate on the birth certificate form whether they want an SSN assigned to their newborn child. When a parent requests an SSN for a child, the State vital statistics office receives the request with the birth registration data from the hospital and then forwards this information to SSA. Under these procedures, the parent is not required to file a separate application for an SSN for the child. Based on the information the State forwards to SSA, we assign an SSN and issue a card for the child.

It is important to note that EAB is a voluntary program on the part of the hospitals and the States and other jurisdictions. No law requires state or hospital participation. The program is administered under the provisions of a contract between each state and SSA. SSA reimburses the states for participation on a per item basis (currently $2.04 for each birth record). EAB is a far more secure way to enumerate newborns. In addition, the program provides significant savings to the Federal government and a convenient service option for the public.

Enumeration at Entry (EAE)

To reduce fraud and improve government efficiency, SSA inaugurated our Enumeration-at-Entry process in October 2002. Under this process, SSA has entered into agreements with DHS and the Department of State (DOS) for those agencies to assist SSA in enumerating aliens. To assist SSA, DOS collects enumeration data as part of the immigration process. When the immigrant enters the United States, DHS notifies SSA and the card is issued.

Social Security Cards

In the beginning of the Social Security program, no special efforts were needed to prevent the Social Security card from being counterfeited. However, as the card's use expanded and technology improved, counterfeiting became a concern. Beginning in 1983, the Social Security Act required that SSN cards be made of banknote paper, and to the maximum extent practicable be a card that cannot be counterfeited. SSA worked with the Bureau of Engraving and Printing, the Secret Service, and the Federal Bureau of Investigation to design a card that met these requirements.

All Social Security cards issued since October 1983 incorporate a number of security features intended to make the card counterfeit-resistant and tamper-proof. Some of these features include, but are not limited to, a tamper-proof marbleized background; Intaglio printing in some areas of the card; and colored planchettes (small discs) randomly displayed on the card. Obviously, while some security features have been made public, other features have not in order to protect the security of the card.

The immigration and welfare reform legislation passed in 1996 required SSA to develop a prototype of a new card as well as study and report on different methods for improving the Social Security card process. In 1997, SSA issued a report to Congress on "Options for Enhancing the Social Security Card," and earlier this year provided the Subcommittee with an update on some of the findings in the report.

As you are aware, the expertise of counterfeiters and the wide availability of state-of-the-art technology make it increasingly difficult to develop and maintain a document that cannot be counterfeited, despite best efforts to guard against such incidents. Therefore, SSA continues to evaluate new technology as it becomes available to determine if additional features should be included.

As required by P.L. 108–458, SSA, in consultation with DHS, has formed a taskforce to establish requirements that will further improve the security of Social Security numbers and cards. Since current law requires the card to be printed on banknote paper, the taskforce is limited to consideration of improvements to this type of card. The taskforce includes representation from DHS and several other agencies, including the Federal Bureau of Investigation, Department of State and the Government Printing Office. The taskforce is considering a wide range of security features that would strengthen the Social Security card, and we will develop a plan for implementing the taskforce recommendations.

The cost of replacing the current SSN card with a new version that includes enhanced security features would depend upon features to be included, e.g. biometric identifiers, and the universe of card-holders needing a new card. The cost of the card itself is minimal. The cost is driven by the cost of verifying the identity of the person applying for the card and, in the case of aliens, determining the immigration status and work authorization.

Last year, we estimated a card with enhanced security features such as biometric identifiers would cost approximately $25.00 per card, not including the start-up investments associated with the purchase of equipment needed to produce and issue

this type of card. While any estimate would ultimately depend on the details of the proposal, last year's estimate for replacing cards for 240 million cardholders nationwide was approximately $9.5 billion. Currently however we know that the cost of issuing SSN cards has increased by approximately $3.00, due to new requirements for additional verification of evidence, so we anticipate an increase in the total cost estimate when we update our figures to reflect current dollar costs.

Legends on the SSN Cards

I would now like to discuss the relationship between the Social Security card and work authorization. The Immigration Reform and Control Act of 1986 (IRCA) makes it illegal for an employer to knowingly hire anyone not legally permitted to work in the United States. Under IRCA, all employers are required to verify the identity and employment eligibility of all new employees regardless of citizenship or national origin. There are a number of documents specified in the law and DHS regulations which may be used for this purpose. Some documents, such as a United States passport, establish both employment eligibility and identity. Others, including a Social Security card without a restrictive legend, can be used to establish employment eligibility but *do not* establish identity and must be accompanied by an identification document, such as a State driver's license.

It is important to note that, just as the Social Security number or card does not establish identity, neither does it always reflect an individual's current work authorization status. The SSN card only reflects an individual's work authorization status at the time the card was issued—it is a snapshot in time. An individual's work authorization status may change over the years, and the DHS has sole jurisdiction over work authorization determinations for noncitizens.

The vast majority of original Social Security cards are issued to United States citizens or to non-citizens who have been permanently authorized to work in the United States. These cards show only the name and SSN of the individual.

Unlike the cards issued to United States citizens or to non-citizens who have been permanently authorized to work in the United States, cards issued to non-citizens who are not authorized to work or who are only temporarily authorized to work bear one of two legends describing work authorization status at the time the card was issued.

"Not Valid for Employment"

Initially, SSA issued the same type of Social Security card to everyone, whether or not the individuals were authorized to work. In 1974, SSA began assigning SSNs for nonwork purposes, but the card was not specifically annotated. Beginning in May 1982, SSA started issuing cards printed with the legend "Not Valid for Employment" to non-citizens who are not authorized to work. This was due to the increasing need for individuals to have SSNs for nonwork purposes and concerns that such individuals might otherwise use their SSNs for work. With this restrictive legend appearing on a card, employers were able, for the first time, to determine whether the individual to whom the card was issued was authorized to work. Of course, an employer could not rely solely on the card to establish that the person presenting the card was the person to whom the SSN was assigned.

Cards containing this legend are often referred to as "nonwork SSNs." In October 2003, SSA significantly tightened the rules concerning issuance of nonwork SSNs. SSA only issues such an SSN when 1)a Federal statute or regulation requires an SSN to receive a particular benefit or service, which an alien has otherwise established entitlement; or 2) a State or local law requires an SSN to get public assistance benefits, to which the alien has otherwise established entitlement and for which all other requirements have been met.

"Valid for Work Only with DHS Authorization"

Beginning in September 1992, SSA began issuing cards with the legend "Valid for Work Only with INS Authorization" to noncitizens lawfully in the United States with temporary authorization to work. This legend has been changed to "Valid for Work Only with DHS Authorization" to reflect the change from "INS" to "DHS". In these cases, employers must look at the non-citizen's DHS documents to determine if the individual has current work authorization. In addition a participating employer may use the DHS employment eligibility verification service, known as the Basic Pilot, to confirm employment eligibility for newly hired employees, which includes verification with SSA records and for noncitizens, with DHS records.

In Fiscal Year (FY) 2005, SSA issued approximately 5.4 million original cards. Of these, 4.3 million were issued to United States citizens. Approximately 1.1 million cards were issued to non-citizens with temporary or permanent work authorization.

Over the years SSA has made continual enhancements to the Social Security card. Because of the substantial cost of replacing all cards in use, older versions of the

card remain valid. Thus, there are about 50 different variations of the SSN card that have been issued since 1936.

NonWork SSNs

SSA also issues cards to aliens legally in the United States but who are not authorized to work by DHS. Last year SSA issued fewer than 15,000 of this type of non-work card. Each year as required by Section 414 of the Illegal Immigration Reform Act of 1996, P.L. 104–208, SSA reports to Congress the number of SSNs assigned to aliens who were not authorized to work in the United States when the card was issued for whom we receive Form W–2s. The most recent report stated that earnings were credited to 555,227 SSNs assigned to non-citizens who did not have authority to work in the United States at the time the SSN was assigned. It is important to note that since the work authorization status of a non-citizen may change, an earnings report under a nonwork SSN does not necessarily mean that unauthorized work was performed.

Additional Efforts to Strengthen the Enumeration Process

SSA has taken a number of steps to further strengthen the processes associated with assigning SSNs. You will recall that SSA formed a high-level response team to develop recommendations on enumeration policy and procedure in the aftermath of the terrorist attacks of September 11, 2001. As previously reported to this Subcommittee, implementation of many of the team's recommendations has strengthened our capability to prevent those with criminal intent from obtaining and using SSNs and SSN cards. As mentioned earlier in my testimony, beginning June 1, 2002, SSA began verifying birth records with the issuing agency for all United States born SSN applicants age one or older. In addition, beginning in July 2002, SSA began verifying the authenticity of all immigration status with DHS before assigning SSNs to non-citizens.

We also continue to look for additional ways to make the enumeration process more efficient and secure. In November 2002, SSA piloted a Social Security Card Center in Brooklyn, New York. The Card Center represents a joint effort by SSA, SSA's Office of the Inspector General (OIG) and Department of Homeland Security (DHS). The collaboration of these parties is intended to strengthen SSN application procedures, and to ensure that applications are processed with a high degree of integrity, efficiency and expertise.

In April 2005, SSA established another Social Security Card Center in Las Vegas, Nevada. The Las Vegas Social Security Card Center is dedicated exclusively to helping Las Vegas Valley and southern Nevada residents apply for a new or replacement Social Security Card. SSA plans to open additional centers as resources permit over the next several years based on SSN workloads and other service delivery factors.

SSN Verification Processes

Many diverse organizations request SSN verifications for various purposes. SSA must consider each request to determine whether to deny or permit verification and what information, if any, may be disclosed. SSA also must consider each request to ensure that the proper safeguards are in place to protect the information being disclosed. SSA must also be reimbursed for any work not related to the administration of our programs. Of course, by law, we cannot fulfill requests for non-program purposes if doing so would impede our mission.

For many years, most SSN verifications were processed in our field offices. This was a manual process which was highly labor intensive. In 1983, SSA implemented the Employee Verification Service (EVS) in order to better manage the verification workloads. Since then SSA has provided additional ways to access SSN verification routines as technology has evolved.

Employers

Employers are our primary requestors for SSN verifications because they must accurately report wage information for the people they employ. One of SSA's core business processes is maintaining the accuracy of earnings for all workers to ensure that they receive credit for the work on which FICA taxes were paid. Accurate earnings information is important because a worker's earnings record is the basis for computing retirement, survivors, and disability benefits.

SSA has successfully provided SSN verification services to the employer community for many years. Employers can verify SSNs for their employees by telephone, by submitting paper listings or by magnetic media.

To further improve our service to employers, SSA piloted an online service, known as Social Security Number Verification Service (SSNVS), in April 2002. In June 2005, SSA expanded the availability of this service to all employers. This optional,

free and secure Internet service provides employers with an immediate response for a limited number of SSN verification requests or a next business day response for high volume SSN verification requests.

As mentioned earlier in my testimony, employers may participate in the Basic Pilot program, an ongoing joint initiative in which SSA supports DHS in assisting participating employers in confirming employment eligibility for newly hired employees. Participating employers may use the automated system to verify SSNs and alien registration or admission numbers through verification checks of SSA and DHS databases.

In 2005, through the EVS, SSNVS, and Basic Pilot programs, we estimate we provided a total of 67 million employer verifications, up from 62 million in 2004.

Federal and State Agencies

Many Federal, State, and local agencies request SSN verification services for numerous purposes, from issuing food stamps to tracking convicted felons. Some of the agencies receive information as a result of legislation. Some of these organizations include, but are not limited to:

- The Department of Education
- The Department of Justice
- The Office of Child Support Enforcement
- The Internal Revenue Service
- The Department of Veterans Affairs
- The Selective Service System
- Any Federal agency which uses the SSN as a numerical identifier in their record system
- Federal, State, and local agencies for validating the SSN used in administering income or health maintenance programs
- Federal, State, and local agencies where SSN use is authorized under Federal statute and they are involved in programs such as Temporary Assistance for Needy Families, Food Stamps, Medicaid, and Unemployment Insurance
- State Motor Vehicle Agencies
- Prisons
- Law enforcement fugitive felon operations
- SSA OIG.

SSA provides verifications to some State agencies, such as State motor vehicle licensing agencies via the American Association of Motor Vehicle Administrators (AAMVA).

Third Parties

Under the Privacy Act, SSA may verify or release SSNs to third parties that have obtained the written consent of the number holder, regardless of the purpose of the request. SSA has been providing such third party verifications for many years through existing verification processes.

Impact of Public Law 108–458

Section 7213 of P.L. 108–458 contains several provisions to strengthen the integrity of our enumeration process. Two key provisions include the implementation of limits on the number of replacement SSN cards an individual can receive to three per year and ten per lifetime with limited exceptions and the addition of death and fraud indicators to SSN verification routines for employers, State agencies issuing driver's licenses and identity cards, and other verification routines as determined to be appropriate.

As I mentioned previously, SSA implemented the restrictions on replacement SSN cards effective December 17, 2005 as required by IRTPA. In addition, although most death records were already available to employers and DMVs through our SSN verification services, we have also added the State death records that were previously restricted as authorized by IRTPA. Those additional death records were added to SSN verification routines on March 6, 2006, well before the implementation deadline set by IRTPA. We continue to work to ensure that fraud indicators will be added to the SSN verification routines by December 2007.

Section 7213 of IRTPA also required SSA to establish minimum standards for verification of documents submitted in connection with an SSN. To this end, SSA established rigorous new standards for evidence of U.S. citizenship and identity submitted in connection with an application for an SSN.

IRTPA also required SSA to form an interagency taskforce specifically charged with establishing security requirements, including standards for safeguarding SSN cards from counterfeiting, tampering, alteration and theft. This interagency taskforce is working to improve the security features included on the current bank-

note card. SSA will prepare for implementation of the taskforce recommendations by June 2006.

Conclusion

In conclusion, the Social Security number was originally intended as a means to provide a record of the earnings of people who worked in jobs covered under the new Social Security program. We must remember that with all the improvements in the assignment of SSNs, the Social Security card is still just a record of the SSN assigned to the individual and not an identity document.

However, as we all know, the use of the SSN for other purposes has grown significantly over the years. The challenge we face is to balance SSA's commitment to assigning numbers quickly and accurately to individuals who qualify for them and need them to work, with the equally important need to maintain the integrity of the enumeration system to prevent SSN fraud and misuse.

I want to thank the Chairman and members of the Subcommittee for inviting me here today, and I look forward to working with you to continue to improve SSA's processes.

I will be happy to answer any questions you might have.

Chairman MCCRERY. Thank you, Mr. Streckewald. Dr. Kent.

STATEMENT OF STEPHEN T. KENT, VICE PRESIDENT AND CHIEF SCIENTIST, INFORMATION SECURITY, BBN TECHNOLOGIES; AND CHAIRMAN, COMMITTEE ON AUTHENTICATION TECHNOLOGIES AND THEIR PRIVACY IMPLICATIONS, NATIONAL RESEARCH COUNCIL, THE NATIONAL ACADEMIES

Dr. KENT. Good morning, Chairman McCrery, Congressman Levin. I am Steve Kent, Vice President and Chief Scientist, for Information Security at BBN Technologies. I served as the Chair of the Committee on Authentication Technologies and their Privacy Implications for the National Research Council, the operating arm of the National Academy of Sciences.

The study Committee authored two reports: "IDs, Not That Easy, Questions About Nationwide Identity Systems," on which you have asked me to testify, and "Who Goes There: Authentication Through The Lens Of Privacy." It is a pleasure to be here to discuss these reports with you. I will try to briefly summarize my written testimony which I submitted for the record.

First, some general observations: developing identity systems is much more complex than it initially appears. Several key policy questions must first be answered, among them what problem is the system supposed to solve, and how will it try to solve the problem? How authentication will be achieved has to be looked at; who would be users of the system, who will rely on it, what types of uses will be allowed, and what legal structures protect the integrity of a system.

Implicit in all these are that we are dealing with a system, not just ID cards. Success, therefore, depends not only on the card technology we use but on all of the ways the system components have to work together. The high cost of fixing or even abandoning a system makes it essential that potential ramifications are explored very thoroughly prior to making decisions about design details and deployment of a system.

Let me address a few of the specific questions that you posed. There are a number of technical challenges associated with building a counterfeit resistant, long lasting, easily replaceable ID card.

No method of ensuring that the person presenting the card is the proper owner can be completely reliable. A key decision for any system of this sort would be determining an acceptable threshold of false rejection and false acceptances, none of which are going to be zero in any practical technology.

Second, any large scale identity system designed for a specific purpose is almost always used for other, secondary purposes. The ID may be used for verification unrelated to the original purposes. The data collected may be used in ways that have little to do with the original purpose.

These unplanned uses often cause problems. For example, security and privacy protections that were designed for the original use might not align with the needs of a secondary use. Data collected for the primary use might not be appropriate in terms of quality or reliability for a secondary use.

For the primary user, the existence of secondary uses can make it difficult to respond to a detected attack on the system. The range of possible reasons for the attack grows with secondary uses, making it more difficult to determine how to respond. The ID system databases hacked, for instance, was in an individual trying to get a fake ID for purchasing alcohol or someone with more nefarious purposes in mind.

Third, the privacy implications of large scale identity systems are significant. A major challenge to privacy is the ability to cross-reference databases in different systems tied to an ID, even when the primary system is privacy-preserving. Another problem is that of identity theft. To lessen the impact on privacy, a number of steps can be taken, including being clear about the system's purpose, minimizing the scope and retention of collected data, and clarifying who will have access to data, and, of course, providing means for individuals to check on and correct information stored about them to rectify errors in the system.

Fourth, identity establishment itself is a challenging but critical part of the process. Of particular concern is the fact that fundamental documents, foundational documents like birth certificates that are required to establish identity for other identity documents are themselves subject to fraud and forgery.

Moving to digital credentials or biometrics will not change some of the basic avenues of attack against a large scale identity system. As a result, the issuing process itself will remain extremely vulnerable. The best any new system can provide is a compelling connection with some previous verification of identity, and that is usually imperfect.

Finally, while our reports did not address the specific concerns you asked about with regard to modifying the SSN card to help prevent unauthorized immigrants from gaining lawful employment, the framework we presented in our study I think can be applied to this topic.

It is important to note that layering a new system on top of the primary use of the SSN card would not intrinsically add to the testimony of the data that was collected for that original purpose. The data has the same quality and reliability that it had prior to the addition of the new system and the introduction of higher quality credentials in a physical sense.

In conclusion, as the title of our report suggested, IDs, Not That Easy, none of the issues raised by development and deployment of large scale identity systems are simple. The questions posed in our report should be carefully and thoroughly applied, not only from a privacy perspective but from a security, usability and effectiveness perspective as well.

Thank you. That concludes my comments. I will be happy to take any questions.

[The prepared statement of Dr. Kent follows:]

Statement of Stephen T. Kent, Ph.D., Chairman, Committee on Authentication Technologies and Their Privacy Implications, National Research Council, The National Academies

Good morning, Mr. Chairman and members of the Committee. My name is Stephen Kent. I am Vice President and Chief Scientist for Information Security at BBN Technologies and served as the chair of the Committee on Authentication Technologies and Their Privacy Implications of the National Research Council. This study committee authored the two reports, *IDs—Not That Easy: Questions About Nationwide Identity Systems and Who Goes There? Authentication Through the Lens of Privacy*, on which you have asked me to testify. The National Research Council is the operating arm of the National Academy of Sciences, National Academy of Engineering, and the Institute of Medicine of the National Academies, chartered by Congress in 1863 to advise the government on matters of science and technology.

It is a pleasure to be here to discuss these reports on large-scale identity systems. By way of background: the study committee originally planned to do only the *Who Goes There?* report. We decided on the *IDs* report about half-way through our study process after the September 11, 2001 terrorist attacks. In the wake of those attacks, numerous proposals for what identity systems could or should accomplish with respect to counterterrorism began circulating in the policy community and the media. The study committee believed that the persistence of public discussion about possible new ID systems and the expectation that other proposals would continue to be offered argued for an informed analysis and critique of the concept of a nationwide or large-scale identity system. The brief report on IDs was the result. It was intended to catalyze a broader discussion, and I am happy to be here today to continue that discussion.

I will start with a brief overview of the highlights of the *IDs* report and then address some of the specific issues that you asked me to consider in my testimony today.

Perhaps the most important message of our work on ID systems is that designing and building systems to ascertain identity is much more complex than it might appear and is indeed why we titled our *IDs* report "Not That Easy."

A primary consideration is to understand the goals of a large-scale identity system. Before any decisions can be made about *whether* to attempt some kind of system, the question of precisely *what* is being discussed and what purpose it will serve must be answered. What problem or problems is the proposed system meant to solve? The high-level policy questions that the *IDs* report outlines include the following:

- What is the purpose of the system? What problem or problems is it attempting to address?
- What is the scope of the population that would be issued an ID? Related to this, how would the identities of these individuals be authenticated?
- What is the scope of the data that would be gathered about individuals in support of issuing an ID and how would it be correlated to data about them in any databases associated with the system?
- Who would be the users of the system? By this we mean not only those who would be issued an ID, but the government agencies, perhaps state and local governments, or even the private sector organizations that might rely on the IDs. What entities would be allowed to use the system? Who could contribute, view, and/or edit the data in the system?
- What types of use would be allowed? Who could demand an ID? Under what circumstances? What types of database queries about individuals would be permitted? Would data mining or analysis of the information collected be permitted? Who would be allowed to do such analysis? For what purposes?

- Would enrollment in and/or identification by the system (even if the individual had not formally been enrolled) be mandatory or voluntary?
- What legal structures protect the system's integrity as well as the ID holder's privacy and due process rights? What structures determine the government and relying parties' liability for system misuse or failure?

Answers to all of these questions (and more) will have ramifications for the technological underpinnings of the system, including what levels and kinds of system security will be required.

Implicit in all of these questions is the notion of a "system" and not merely an "ID card." The fact that any identity management proposal necessarily implies a "system" may be one of the most important (and less discussed) aspects of many of the identity system proposals that we have seen. These systems, at the scale that they are proposed, necessarily imply the linking together of many social, legal, and technological components in complex and interdependent ways. The success or failure of such a system is dependent not just on the individual components (for example, the ID cards that are used, or the biometric readers put in place) but on the ways they work, or do not work, together. For example, are card readers located where they need to be? How well do the readers operate under various environmental and load scenarios? Who will operate the systems and how will they be trained and vetted? Do enrollment policies align with the security needs envisioned for the system? And so on. How well these interdependencies are controlled along with the mitigation of security vulnerabilities and the unintended consequences of the deployment of a system, will be critical factors in its overall effectiveness.

In addition to the questions above, the committee outlined several cautions to bear in mind when considering the deployment of a large-scale identity system:

- Given the costs, design challenges, and risks to security and privacy, there should be broad agreement in advance on what problem or problems the system would address.
- The goals of the system should be clearly and publicly identified and agreed upon, with input sought from all stakeholders.
- Care must be taken to explore completely the potential ramifications of deploying a large-scale identity system, because the costs of fixing, redesigning, or even abandoning a system after broad deployment would likely be extremely high.

That is a brief overview of some of the highlights from the *IDs* report. The study committee urged that proponents of large-scale identity systems present a compelling case addressing the issues raised in these reports and solicit input from a broad range of stakeholder communities. The *IDs* report elaborates on these issues and also considers some of the technological and security challenges inherent in large-scale identity systems. Some of the issues you asked me to address in my testimony today are more specific than what I have presented here so far, and to the extent that our reports address them, I will briefly discuss them.

Tamper-Proof ID Cards

Cards are often suggested as a means of binding an "identity" within a system to an individual. The question being: if someone presents a valid card, how do you know first, that the card is valid, and second, that the card belongs to the person presenting it? To the first question, the goal of a counterfeit-resistant, long-lasting, easily-replaceable ID card presents difficult technical challenges. Magnetic stripe cards are trivially easy to counterfeit. Memory cards or smart cards are more difficult, but not impossible, to duplicate or forge. Use of cryptographic technologies and digital signatures can help, but for any technology, some degree of imperfection will exist. I have already mentioned that a key notion to keep in mind is that these systems are in fact *systems*—they would likely encompass databases, processes and procedures, cards, card readers, architectural requirements, security needs, and much more, not to mention the *people* who are a part of any technical system. Any ID card that is issued is only a component of the system. One question that must always be asked is what is the perceived threat? By threat I mean what set of adversaries do we believe we need to thwart, what are their capabilities, and what are their goals? If we cannot answer that question, we have no rational basis for deciding if any proposed system will likely be adequate, or whether it will be overkill.

To the question of ensuring that the person presenting the card is the same person identified with the card, a picture on the front of the card might be some assurance, but people sometimes have a hard time matching faces to pictures. "Two-factor authentication" in which an individual presents a card along with additional information (such as a PIN or thumbprint—either of which could be compared to data

on the card) is another possibility. Another scenario might be to have the person interact with a biometric scanner and present the card that contains reference information for the biometric in question. Both pieces of information are validated in combination against a backend server. This, however, creates a requirement for high availability and a dependence on a secure, reliable network and communications infrastructure. Also, unless the scanner is itself a secure device (and known to be so through some kind of formal evaluation process) or the scanner is closely monitored, the system may be compromised. Even then, the system will not be fool-proof. (I am informed, by the way, that the NRC is conducting a large study on biometric systems that should be released later this year)

A decision on thresholds for false rejection and false acceptance rates (which is, first, a policy decision) will need to be made—and those thresholds cannot really be zero for any technology. Moreover, even the best-designed systems are subject to social engineering (there are numerous examples of personnel being tricked into issuing credentials without adequate proof of identity or authorization) and insider threat attacks—and thus one cannot rely on technological solutions alone. The entire system and implications of policy decisions at all levels must be thought through carefully.

Secondary Uses

One of the challenges that arises repeatedly with a large-scale identity system designed for a specific purpose (or set of purposes) is that there are almost always forces in play that push the systems to be used for things that they were not originally designed for. A familiar example of this is the state driver's license, which does not merely enable one to legally drive on public roads, but is also relied on to provide "proof of age" for alcohol purchases and "proof of identity" to board an aircraft for domestic travel in the U.S.

Most systems do not explicitly guard against secondary uses, although occasionally there are legal requirements or contractual relationships that limit secondary use (such as credit card agreements.) There are at least two ways in which secondary use might happen. In some cases, *the card* presented may be used for additional verification purposes in contexts unrelated to the original purposes. In other instances, *the data* collected in support of card issuance may be used in ways that have little to do with the original purpose. Unintended uses of an identity system and its associated technologies can always have inadvertent side effects. There are numerous examples in the literature of this, and the expansion over time in use of the Social Security Number (SSN) is a well-known instance. For example, the proposed ID might become the new, de facto photo ID for individuals, potentially exposing SSNs to a very wide range of organizations at a time when states are eliminating the SSN from driver's licenses.

If any new ID system is deployed, chances are that there will be uses found for it that were not originally intended. While this might seem an efficiency on the surface, in fact, such unplanned-for multiple uses may cause problems.

- A particular challenge resulting from unplanned-for uses is when technology or an ID system designed for a specific security context, user population, and so on is used (intentionally or unintentionally) without a determination as to whether the original security, privacy, and usage assumptions still hold in the new context. Secondary uses are implicitly relying on whatever assurances, security models, and privacy protections the original designers and implementers were working with. These may not align with the needs of the secondary user. For example, access to a health club may require a different usability or privacy model than access to secured facilities at an airport. One size cannot fit all.
- A significant context consideration is the security of the system. The original system was designed with a particular threat model in mind; this threat model may not apply to secondary uses of the system.
- Another problem is that the data collected for the original purposes may not be what is needed, or at the appropriate quality or reliability levels, for the new secondary uses.
- Depending on inappropriate assumptions is not a challenge just for the secondary user, but also for the primary users of the system. An ID system that is used for multiple purposes with multiple types of threats, not all of which were designed or planned for, can make it difficult to respond to a known attack on the system. This is because with secondary uses, the universe of possible motivations behind the attack is much larger, making it difficult to ascertain what is an appropriate response to an attack. If your database is hacked, was it individuals desiring a fake ID to purchase alcohol, for example, or individuals with more nefarious purposes in mind?

Privacy Consequences

The privacy implications of large-scale identity systems can be significant. While casual discussions of IDs or ID cards may assume simple, unique pairings of information and individuals, the reality is often more complicated. A major privacy challenge, even when a given system has been designed and is operating in a secure and privacy-sensitive fashion, is the ability to cross-reference and link information across databases in different systems. In many cases, an identity in a given system will include a common cross-reference, such as a Social Security Number, that makes it trivially easy to link it to other identities associated with other systems (presumably designed for other purposes.) In addition, questions arise as to how reliable the linking would be—some institutions may not mind if suggested linkages are only approximate (for example, a vendor attempting to do targeted marketing), whereas others demand high levels of accuracy.

Identity theft is also a major concern, especially in the case of centralized databases or systems used for multiple purposes—the more useful or "powerful" an ID is the more tempting it is as a target. Identity theft is an individual's fraudulent claim that he or she is the person to whom the information in the system refers, allowing him or her to derive some benefit from another party who is relying on that claim. One reason for the problem is the expanded use of SSNs for purposes that were not originally intended coupled with the assumption that they are 'secret' or should act as a 'key.'

When designing a system to lessen impacts on personal privacy, the study committee made a number of recommendations, including:

- Be clear about the purposes of the system.
- Minimize the scope of the data collected to that which is essential for the purpose of the ID system.
- Minimize the retention interval for data collected in association with use of the card.
- Clarify who will have access to the collected data.
- Clarify what kinds of access to and use of the data are allowed.
- Ensure that use of the system is audited to protect against illegitimate uses as well as to monitor for security threats.
- Provide means for individuals to check on and correct the information stored about them.

All of that said, many times there are important uses of data that are unanticipated when the data are collected. For these as for other important uses, it is a question of balancing the risks to privacy and confidentiality against the benefits of the uses, especially when the uses are for research to inform public policies or for national security. The Academies have long studied the issues here for important research uses of data. A recent study is *Expanding Access to Research Data: Reconciling Risks and Opportunities* from the Academies' Committee on National Statistics. For the case of national security purposes, the Computer Science and Telecommunications Board has joined with the Committee on Law and Justice and the Committee on National Statistics to launch a major study to balance the risks and benefits. The Academies would be pleased to offer more information on these and other studies that may be relevant to your inquiry or to help with further investigations of interest to you.

Identity Establishment

The establishment of an identity in an identity-system is another challenging but critical part of the process. There is a tangled web of government-issued identity documents used as foundational documents that allow the government and other organizations to issue other identity documents. Many of these foundational documents, used to acquire an SSN or Passport, for example, are subject to fraud and forgery themselves. Birth certificates are particularly problematic, in that they are issued by thousands of different jurisdictions across the country, making them both easy to forge and difficult to verify and thus very poor to use as an identification document from a security perspective. Moreover, no aspect of a birth certificate binds it to an individual in any strong security sense. The types of possible attacks on identity documents vary and include the following:

- An individual acting as an impostor.
- Forged or fraudulent documents.
- Tampering with existing documents.
- Compromise of confidential information (for example, in an identity system database) that is then used to create a false identity.
- Modification of computerized records to support a false identity.

Moving to, for example, digital credentials or biometrics will not change these basic avenues of attack and fraud. As technology and perhaps ID cards become ever more sophisticated, the issuing process will remain extremely important. All the security in the world cannot overcome deficiencies in this step—the system will only be as good as the data that goes into it. The best that any system can provide is a compelling connection with some *previous* verification of identity. Essentially, trust in the integrity of the system is based not so much on any single verification when an individual presents a claim of identity as it is on increasing confidence when multiple transactions happen over time and all previous transactions with that particular individual have worked out.

Other Questions

You asked me to comment in particular on the issue of modifying the SSN card so that it is tamper- and counterfeit-resistant as part of efforts to prevent unauthorized immigrants from gaining lawful employment in the United States. While the National Research Council's reports did not address this specific question, such an approach clearly falls within the realm of large-scale identity systems that the study committee was considering. The framework that we presented can be applied to this question.

For example, once the purpose of a system is clearly articulated—in this case the prevention of unauthorized people from gaining lawful employment in the United States—then a next question to ask is what information would accomplish the goal of ascertaining whether an individual is qualified to work in the United States? Who has that data? Who collects it? Who can access it? If a system with that sort of data were deployed, how would it be regulated? What penalties or liabilities would be associated with misuse? How could individuals correct their own data within the system? What kinds of security would be needed? What are the likely threat models for such a system? How could potential threats of identity theft (in this case "worker-identity") be mitigated? Who would be authorized to ask to see the ID card associated with this system? Are there other likely abuses and how could the possibility of those be mitigated? If the system is to be built on top of another existing identity system (such as the SSN)—which poses its own very serious challenges since this basically would be an unintended, unplanned-for, not designed-for use of the SSN—then what can be assumed about the underlying data in the current system? Layering even the best current security on top of old data only gives the old data an appearance of being more trustworthy—the data has the same quality and reliability that it had prior to the security being added.

Conclusion

Mr. Chairman and members of the committee, our study committee wrestled with questions of identity, authentication, identification, and large identity systems for many months—not new issues, but ones that were brought into sharp focus after September 11, 2001. In the study I have described, we have attempted to lay out our thinking and analysis of these issues. As the report title, *IDs—Not That Easy,* suggests, none of these issues is simple, and any large-scale identity system poses numerous questions that should be carefully thought through—not only from a privacy perspective, but also from security, usability, and effectiveness perspectives. Our reports attempt to lay out some of these questions that must be addressed and to illustrate the complexities that can arise.

You can find more information about these and related studies on the Web site of the Computer Science and Telecommunications Board of the National Research Council at http://www.cstb.org.

Thank you. That concludes my comments. I would be happy to take any questions you may have.

Chairman MCCRERY. Thank you, Dr. Kent. Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, PRESIDENT AND EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you, Mr. Chairman, Congressman Levin. Thank you for the opportunity to testify. My name is Marc Rotenberg. I am President of the Electronic Privacy Information Center. We are a public interest research group here in Wash-

ington. We have done a lot of work related to the SSN. I also teach privacy law at Georgetown Law Center.

I would like to briefly summarize my testimony and ask that the statement be included in the record.

The key points I would like to make this morning concern the history of the effort to restrict the use of the SSN precisely so that it would not form the basis for a national identity card. As you well know, when the number was first established for the purpose of accounting for the SSA contributions, the first regulation that was issued by the the SSA was to make clear that this was not a card for identification purposes.

Now, the particular concern about the possible misuse of the SSN was taken up in 1973 in a very important report by the U.S. Department of Health, Education, and Welfare. This report more than 30 years ago identified the possible misuse of the SSN to link together record systems across government agencies and with private sector record systems.

As a consequence of that investigation, Congress enacted in 1974 the Privacy Act (P.L. 93–579). The Privacy Act, among the various things that it did, set out clear prohibitions on the collection and use of the SSN. Although people at that point in time did not use the phrase identity theft, I think it was a very wise decision on the part of the Congress to limit the use of the SSN, because what we have seen now, 30 years later, is that the broad dissemination of the Social Security number within the United States has contributed to what is now the number one crime. The crime of identity theft is a $53 billion crime, according to a 2004 report of the U.S. Federal Trade Commission (FTC).

Now, since the passage of the Privacy Act, it is obviously the case that the uses of the SSN have expanded by both government agencies and in the private sector, but I think it is important to note at the same time that the Congress and the States and the FTC have taken measures to try to limit the use of the SSN, recognizing that it does create an increased risk of identity theft. I think one of the witnesses spoke earlier about the provision that in effect took the SSN off the State driver's license so that the driver's license would not become the link to other record systems.

Now, certainly, steps can be taken to enhance the Social Security card so that the likelihood of counterfeiting and tampering are diminished, and I think everyone including privacy organizations would favor those measures. The concern here on the privacy side is that the number becomes the basis for linking together different record systems; so, for example, if it becomes the basis for employment eligibility determinations, which could be made by DHS, every employee in the United States, not just immigrants to this country, would be required to present their Social Security card as a condition of establishing eligibility for employment, and I think this is something that was clearly never anticipated in the use of the number. I very much support the testimony of Dr. Kent and the work of the National Research Council.

As these uses are expanded to determine citizenship, for example, or to determine employment eligibility, the increasing risks of misuse expand as well, as do the targets of opportunity and incen-

tives for people to take advantage of the SSN and use it in ways that will cause actual harm and crime to individuals.

So, our recommendation to you today, particularly in the context of a series of hearings that look at high risk issues associated with the use of the SSN, is to ensure that there are adequate security and privacy safeguards for current uses and to avoid new uses that might introduce new risks and new dangers to American consumers.

There is a good reason, I believe, that people in this country in particular are very uneasy about a national identity card, and it is part of our longstanding traditional that we would not, as a general matter, expect to live in a country where the government could say in effect please present your identity and prove to us who you are.

Thank you very much for the opportunity to testify this morning.

[The prepared statement of Mr. Rotenberg follows:]

Statement of Marc Rotenberg, President, Electronic Privacy Information Center

Introduction

Chairman McCrery, Ranking Member Levin, and Members of the Subcommittee, thank you for the opportunity to testify on the high-risk issues surrounding Social Security numbers.

My name is Marc Rotenberg and I am Executive Director of the Electronic Privacy Information Center. EPIC is a non-partisan research organization based in Washington, D.C.[1] Founded in 1994, EPIC has participated in leading cases involving the privacy of the Social Security Number (SSN) and has frequently testified in Congress about the need to establish privacy safeguards for the Social Security Number to prevent the misuse of personal information.[2] Last year, I testified on H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act of 2005 and urged Members to reject the use of the SSN as a national identifier and to ensure the development of adequate privacy and security safeguard to address the growing crisis of identity theft.[3]

Social Security numbers have become a classic example of "mission creep," where a program designed for a specific, limited purpose has been transformed for additional, unintended purposes, some times with disastrous results. The pervasiveness of the SSN and its use to both identify and authenticate individuals threatens privacy and financial security. Recent efforts to expand employment verification programs based upon SSN identification would turn the SSN into a national identifier, subjecting Americans to a national tracking systems and also heightening the risks of identity theft. There are additional risks associated with some of the technological features that the proponents of an "upgraded" Social Security card have suggested. As the New York Times reported yesterday, RFID chips that are being added to identity cards including the U.S. passport, are apparently subject to computer vi-

---

[1] EPIC maintains an archive of information about the SSN online at http://www.epic.org/privacy/ssn/.

[2] *See, e.g., Greidinger v. Davis,* 988 F.2d 1344 (4th Cir. 1993) ("Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling"); *Beacon Journal v. Akron,* 70 Ohio St. 3d 605 (Ohio 1994) ("the high potential for fraud and victimization caused by the unchecked release of city employee SSNs outweighs the minimal information about governmental processes gained through the release of the SSNs"); Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, at a Joint Hearing on Social Security Numbers and Identity Theft, Joint Hearing Before the House Financial Services Subcommittee on Oversight and Investigations and the House Ways and Means Subcommittee on Social Security (Nov. 8, 2001) *available at* http://www.epic.org/privacy/ssn/testimony_11_08_2001.html; Testimony of Chris Jay Hoofnagle, Legislative Counsel, EPIC, at a Joint Hearing on Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves Before the House Ways and Means Subcommittee on Social Security and the House Judiciary Subcommittee on Immigration, Border Security, and Claims (Sept. 19, 2002) *available at* http://www.epic.org/privacy/ssn/ssntestimony 9.19.02.html.

[3] Testimony of Marc Rotenberg, President, Electronic Privacy Information Center, at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005" before the House Judiciary Committee Subcommittee on Immigration, Border Security, and Claims (May 12, 2005) *available at* http://www.epic.org/privacy/ssn/51205.pdf.

ruses and other forms of attack.[4] These risks associated with the expanded use of the Social Security Number and identification cards underscore the importance of the hearing today.

History of SSN Use

The Social Security Number (SSN) was created in 1936 for the purpose of administering the Social Security laws. SSNs were intended solely to track workers' contributions to the social security fund. Legislators and the public were immediately distrustful of such a tracking system, which can be used to index a vast amount of personal information and track the behavior of citizens. Public concern over the potential abuse of the SSN was so high that the first regulation issued by the new Social Security Board declared that the SSN was for the exclusive use of the Social Security system.

Over time, however, legislation allowed the SSN to be used for purposes unrelated to the administration of the Social Security system. For example, in 1961 Congress authorized the Internal Revenue Service to use SSNs as taxpayer identification numbers.

A major government report on privacy in 1973 outlined many of the concerns with the use and misuse of the Social Security Number that show a striking resemblance to the problems we face today. Although the term "identify theft" was not yet in use, *Records Computers and the Rights of Citizens* described the risks of a "Standard Universal Identifier," how the number was promoting invasive profiling, and that many of the uses were clearly inconsistent with the original purpose of the 1936 Act. The report recommended several limitations on the use of the SSN and specifically said that legislation should be adopted "prohibiting use of an SSN, or any number represented as an SSN for promotional or commercial purposes."[5]

In enacting the landmark Privacy Act of 1974, Congress recognized the dangers of widespread use of SSNs as universal identifiers, and enacted provisions to limit the uses of the SSN. The Senate Committee report stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." Short of prohibiting the use of the SSN outright, Section 7 of the Privacy Act provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." This provision attempts to limit the use of the number to only those purposes where there is clear legal authority to collect the SSN. It was hoped that citizens, fully informed that the disclosure was not required by law and facing no loss of opportunity in failing to provide the SSN, would be unlikely to provide an SSN and institutions would not pursue the SSN as a form of identification.

The SSN as a National ID Number Erodes Privacy

Contrary to the clear intent of the Privacy Act, legislation considered this term has proposed to build the SSN and the Social Security card into a national ID. H.R. 98, for example, would create a *de facto* national identity card. Despite any disclaimers that the card was not to be used for identification, employers required to verify the information on the card (which would bear a photograph and a machine-readable unique identifier) would likely rely upon these "fraud prevention measures" as practical identification requirements. It is important to note that the SSN and its basic card are not intended to be used for authentication and identification purposes today, and yet far too many entities rely upon it for just those purposes. Adding the trappings of an identification document to it, including photographs and machine-readable technology, only reinforces the card's status as a badge of identity.

Furthermore, using the SSN for employment verification would necessarily require the building of a vast database of nearly all people employed within the country, which could be easily indexed and correlated with other databases via the SSN. It is precisely this use of the SSN that the drafters of the Privacy Act sought to prevent. H.R. 98 proposed that the database be available to Homeland Security for "any other purpose the Secretary of Homeland Security deems to be an the national security interests of the United States." This vague clause perfectly illustrates "mission creep," and highlights the risk that a national database, based on SSNs, estab-

---

[4] John Markoff, "Study Says Chips in ID Tags Are Vulnerable to Viruses," New York Times, March 15, 2005.

[5] "Records, Computers, and the Rights of Citizens," Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education & Welfare 125–35 (MIT 1973).

lished for one purpose could quickly be transformed into an open-ended system of national surveillance.

A mandatory, national index of all people employed within the U.S. would allow the tracking of individuals on an unprecedented scale. Each person applying for a job would be subject to a status determination by a government agency with each application. In essence, a person's life and livelihood would be determined by a database kept by the federal government—a database grounded in a flawed system of identification never intended for the purpose.

Identity Theft

Nor are the uses of a universal identifier limited to government uses. In fact, it is commercial enterprises that have made the SSN synonymous with an individual's identity. Despite the fact that the cards were never intended to be used for identification purposes, they are considered the "keys to the kingdom" for records about individual consumers.

The financial services sector, for instance, has created a system of files containing personal and financial information on nearly ninety percent of the American adult population, keyed to individuals' SSNs. This information is sold and traded freely, with virtually no legal limitations. This widespread use, combined with lax verification procedures and aggressive credit marketing that lead to widespread identity theft.

Credit grantors rely upon the SSN to authenticate a credit applicant's identity; many cases of identity theft occur when thieves apply using a stolen SSN and their own name. Despite the fact that the names, addresses, or telephone numbers of the thief and victim do not match, accounts are opened and credit granted using only the SSN as a means of authentication. EPIC has detailed many of these cases in other testimony.[6]

The root of this problem is that the SSN is used not only to tell the credit issuer who the applicant is, but also to verify the applicant's identity. This would be like using the exact same series of characters as both the username and password on an email account. The fact that this practice provides little security should not be a surprise.

The printing of SSNs on government-issued drivers licenses provided yet another opening for identity thieves. A thief who stole your wallet could also easily steal your identity, with name, address, diver's license number, and SSN in one easy place. Congress recognized this threat and in the Intelligence Reform and Terrorism Prevention Act of 2004, prevented the printing of SSNs on drivers licenses and other government-issued ID.[7]

International Experiences

The debate on national identification cards is not restricted to the United States. Fierce debates have erupted in other countries over the adoption of national ID cards. The problems presented by such cards in the UK, France, and many other nations are the same problems that we would face here—convenient categorization of individuals' records, to be used or abused by governments or those who obtain access to government records.

The protests against the UK national ID cards are strong, and from esteemed sources such as the London School of Economics,[8] yet they address a system that is even less problematic than one that could use the SSN as a national ID. In the UK, for example, the national ID card would be a voluntary document. And in Ireland, a proposal to establish national was recently rejected.[9] Here in the U.S., SSNs are most frequently assigned at birth. We would be putting in place a system mandating ownership of a machine-readable photo ID, a step that other parts of the

---

[6] *See, e.g., TRW, Inc. v. Andrews,* 534 U.S. 19 (2001) (Credit reporting agencies issued credit reports to identity thief based on SSN match despite address, birth date, and name discrepancies); *Dimezza v. First USA Bank, Inc.,* 103 F. Supp.2d 1296 (D. N.M. 2000) (same). *See also United States v. Peyton,* 353 F.3d 1080 (9th Cir. 2003) (Credit issued based solely on SSN and name, despite clear location discrepancies); *Aylward v. Fleet Bank,* 122 F.3d 616 (8th Cir. 1997) (same); *Vazquez-Garcia v. Trans Union De P.R., Inc.,* 222 F. Supp.2d 150 (D. P.R. 2002) (same).

[7] Pub. L. No. 108–408 §§ 7211–7214, 118 Stat. 3638, 3825–3832 (2004).

[8] London School of Economics, The Identity Report: an assessment of the UK Identity Cards Bill and its implications (2005) *at* http://is2.lse.ac.uk/IDcard/identityreport.pdf.

[9] EPIC prepares an extensive annual survey of international developments concerning privacy protection, including the debates over identity documents. See *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (EPIC 2004), available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-82586&als[theme]=Privacy%20and%20Human%20Rights&headline=PHR2004#_Toc396491834 ("Identity systems").

world, even those less opposed to government interference in personal affairs, seem loath to take.

Measures to Prevent Fraud

The need to present such a card at every employment encounter, and possibly also for homeland security purposes, would also likely increase the need to carry the card on one's person, rolling back the benefits achieved by taking the SSN off of driver's licenses. The reason that the SSN can so easily be used for fraud is not that the card lacks anti-counterfeiting measures; it is the fact that the card is being used as an identifier in so many contexts that it should not be. Efforts to protect the SSN and its holders should therefore be focused upon limiting its uses and disclosures.

Several states have, in recent years, established new privacy protections for SSNs. These laws demonstrate that major government and private sector entities can still operate in environments where disclosure and use of the SSN is limited. They also provide examples of protections that should be considered at the federal level. For example, Colorado, Arizona, and California all have laws that broadly restrict the disclosure and use of the SSN by both government and private actors. These laws encourage agencies and businesses to use different identifiers for their specific purposes, reducing the vulnerability that the disclosure of any one identifier may create.[10] Arizona's law also prohibits the printing of the SSN on material mailed to Arizona residents, reducing the threat of fraud from intercepted correspondence.

Other states, including New York and West Virginia, have statutes that limit the use of the SSN as a student ID number.[11] This reduces the vulnerability of students to identity theft and protecting the privacy of students whose personal information is collected in databases, and whose grades are often publicly posted, indexed by their student ID numbers.Similar laws exist in Arizona, Rhode Island, Wisconsin, and Kentucky.[12]

Congress and this Committee has likewise moved to protect the SSN; just this session, Chairman Shaw and many other members of this Committee introduced legislation that would have added protections on a federal level. We hope that the Committee will be able to act on these proposals this session

These various proposals all tend towards limiting the uses of the SSN, in notable contrast to proposals that expand SSN uses and thus expand individuals' vulnerability. We therefore urge the Committee to regard cautiously any attempt to expand the use of the SSN beyond its already overextended purposes.

Conclusion

The expanded use of the Social Security Number is fueling the increase in identity theft in the United States and placing the privacy of American citizens are great risk. The widespread use of the SSN has made it too easy for government agencies, businesses, and even criminals to create detailed profiles of individuals Americans. Congress wisely sought to limit the use of the Social Security Number when it passed the Privacy Act of 1974, and the states have since established additional safeguards. While new techniques may address some of the security and privacy issues associated with the expanded use of the Social Security card, it clear that these techniques also create new privacy and security risks. We urge the Committee to consider very carefully the high-risk issues associated with the use of the Social Security Number. Every system of identification is subject to error, misuse, and exploitation.

Attachment

Inside Risks: Real ID, Real Trouble?

by Marc Rotenberg

According to the report of the 9/11 Commission, all but one of the 911 1 hijackers acquired some form of U.S. identification, some by fraud. Acquisition of these forms of identification would have assisted them in boarding commercial flights, renting cars, and other activities. As a result, the Commission and some lawmakers concluded it was necessary for the federal government to set technical standards for the issuance of birth certificates and sources of identification, such as driver's licenses. The result was the Real ID Act of 2005.

---

[10] Colo. Rev. Stat § 24–72.3–102; Ariz. Rev. Stat. § 44–1373; Cal. Civ. Code § 1798.85.
[11] N.Y. Educ. Law § 2–b; W. Va. Code Ann. § 18–2–5f.
[12] Ariz. Rev. Stat. § 15–1823; R.I. Gen. Laws § 16–38–5.1; Wis. Stat. Ann. § 36.11(35); Ky. Rev. Stat. Ann. § 156.160.

The new law states that beginning in 2008, "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting the requirements of this section." This means the Department of Homeland Security will issue the technical standards for the issuance of the state driver's license. The practical impact, as CNET explained, is that "Starting three years from now, if you live or work in the United States, you'll need a federally approved ID card to travel on an airplane, open a bank account, collect Social Security payments, or take advantage of nearly any government service." And even some of the more conservative commentators in the U.S. have expressed concerns about "mission creep."

Several objections have been raised about the plan, including privacy and cost, but the most significant concern may be security. As Bruce Schneier has explained, "The biggest risk of a national ID system is the database. Any national ID card assumes the existence of a national database . . . large databases always have errors and outdated information." Even if the identity documents are maintained in the states, problems are likely.

One example concerns the vulnerability of the state agencies that collect the personal information used to produce the license. In 2005, the burglary of a Las Vegas Department of Motor Vehicles put thousands of driver's license holders at risk for identity theft. The information of at least 8,738 license and ID card holders was stolen, and reports of identity theft have already surfaced. Another report uncovered 10 "license-for-bribe" schemes in state DMVs in 2004.

Not surprisingly, the administrators of the state license systems are among those most concerned about the proposal. As the director of Driver Services in Iowa said, "It's one thing to present a document; it's another thing to accept the document as valid. Verifying digital record information is going to be difficult." The National Conference of State Legislatures was more emphatic, "The Real ID Act would cause chaos and backlogs in thousands of state offices across the country, making the nation less secure."

The National Academy of Sciences anticipated many of these challenges in 2002, stating that the U.S. should carefully consider the goals of nationwide ID system: "The goals of a nationwide identification system should be clarified before any proposal moves forward. Proposals should be subject to strict public scrutiny and a thorough engineering review, because the social and economic costs of fixing an ID system after it is in place would be enormous."

The problems of building reliable systems for identification are not unique to the U.S. Many countries are confronting similar questions. In Great Britain, a national debate continues about the creation of a new identity card. The government contends the card is essential for combating crime, illegal immigration, and identity theft, and can be achieved for an operating cost of 584million pounds per year. But a report from the London School of Economics challenged a number of the government positions and a subsequent report found further problems with the ID plan.

The U.K. group concluded, "ID requirements may actually make matters worse." The LSE report cited a recent high-profile breach: "Even as cards are promised to be more secure, attacks become much more sophisticated. Most recently, Russian security agents arrested policemen and civilians suspected of forging Kremlin security passes that guaranteed entrance to President Vladimir Putin's offices."

Systems of identification remain central to many forms of security But designing secure systems that do not introduce new risks is proving more difficult than many policymakers had imagined. Perhaps it's time for the proponents of expanded identification systems to adopt the cautionary line from Hippocrates: "First, do no harm."

Marc Rotenberg (rotenberg@epic.org) is executive director of the Electronic Privacy Information Center (EPIC) and the former director of the ACM Washington Office: an expanded version of this column appears at www.epic.org.

Chairman MCCRERY. Thank you, Mr. Rotenberg, and thank you all for providing excellent testimony and raising some good questions and considerations as we try to sort our way through sometimes conflicting national needs and the desires of our constituents and folks that are concerned about immigration, about illegal immigration, and about terrorism.

We find ourselves kind of going in circles, it seems to me, as we talk about these issues. On the one hand, we all want to protect our border. We want to make sure that people are here legally and working legally, but we also recognize the dangers that Mr. Rotenberg and Dr. Kent pointed out of expanding the uses of the SSN and thereby increasing the opportunity for fraud.

So, it is a complex question, and I appreciate the sunlight that you all have brought to this question. Let us assume for the moment that we could make a card that is much more foolproof than the current card, and that would be very difficult to copy. Even if we had that, let us look at the question of employment eligibility and using that in employment eligibility, because several Members of Congress have already introduced proposals that would require employers to check a government database to confirm an employee's work authorization.

Some of those proposals combine that with an enhanced SSN card that could be used to access the employment eligibility verification system. How effective do you all think such a system would be in preventing unauthorized noncitizens from illegally obtaining employment? Would we get the desired result from the bucks that we expend to put that system in place?

Mr. ROTENBERG. Well, one of the key issues, Mr. Chairman, in that question, and this is also addressed in the National Research Council report, concerns the quality of the underlying data. The proposal which you are referring to, which I think is H.R. 98, would try to, in effect, transform the SSN card into an identity document and enable employers to query a national database, which I believe would be maintained by DHS, to determine the eligibility of a person who is seeking employment in the United States.

It is possible, certainly, to enhance the card through photographs and biometric means to make it into a quasi-identity document. I think it would raise privacy issues, but it would not resolve the question as to the accuracy of the underlying data. I think it is very easy to imagine, particularly with a lot of foreign names, that misspellings and mispronunciations could easily lead to errors in these systems.

Now, that is not necessarily a reason not for doing it, but I think it does underscore the need to, as Dr. Kent said, look beyond the card and to establish this as a system problem and to understand whether or not those databases would support good decisions.

Chairman MCCRERY. Let me just interject for a moment, because we ought not too easily set aside these suggestions in today's world of extremely capable technology. You have mentioned foreign names, and it is easy to get them mixed up. On a computer it is pretty specific. You have to type in exactly the right name. So, if you do that, and you send it to this database, it is not going to get confused; it is going to spit back exactly that name and whether it is authorized or not. So, I do not buy that.

Do you have any other problems that you see with this system being able to correctly identify whether a person in this—I understand the underlying data may be wrong. I do not think we can ever fix that. Well, I do not think as a practical matter we can ever fix that. Assuming that the—well, never mind the underlying data; we can at least say whether the database has this person in it as

authorized to work, can't we? It might be expensive, but we can do that, can we not? These gentlemen are nodding. Dr. Kent.

Dr. KENT. Well, Mr. Chairman, one question that would come to mind immediately is whether everyone would be issued such a credential or only whether people who were immigrants were supposed to have such a credential.

Chairman MCCRERY. That is a good question, and we will get to that.

Dr. KENT. If we assume that only people who were immigrants are supposed to have it, then the burden, I would assume, on the employer is to make an initial determination of whether or not somebody applying for a job is or is not a citizen. Then the question is what existing credentials do they use for that purpose?

If I have to present a birth certificate, then, we encounter all of the residual vulnerabilities associated with birth certificate forgery when people do not go to the extent that the earlier witnesses testified that you can do if you are working hard in a forensic case to deal with fraud or something like that, which the average employer would not be able to do.

So, there are a lot of questions we would have to answer to really be able to determine that.

Chairman MCCRERY. Admittedly, people could find ways to fabricate authentication and thereby get on the database as an authorized worker. Would this system reduce the likelihood that somebody could get a job in the country if that person were here illegally and unauthorized to work?

Dr. KENT. It is hard to say——

Chairman MCCRERY. Sure.

Dr. KENT. —without looking at all the details, but——

Chairman MCCRERY. The next question is how much would it reduce it?

Dr. KENT. Yes.

Chairman MCCRERY. That is an easy question to answer. Sure it would, but would the bang for the buck be worth it? That is the real question.

Dr. KENT. I think that is where an extensive study needs to be undertaken to try to predict whether or not you would be getting, as you say, good bang for the buck out of such a system.

Chairman MCCRERY. Mr. O'Carroll, Mr. Outland, do you have thoughts on this?

Mr. O'CARROLL. Yes, Mr. Chairman, it's sort of a twofold question, the first part asking in terms of designing a card that would be tamper-resistant, difficult to counterfeit, whatever.

What we are finding is basically anything that has been engineered can be reengineered, and that is kind of our take on any of the expense that would go into coming up with a more counterfeit-proof card. It is really going to be pretty difficult, and the result on it is probably not going to be as good as one would hope.

So, what we are kind of in agreement with you on is that it is the underlying data that is the most important. Right now, what Social Security is using with DHS as the basic pilot, the SSA is verifying the SSN. The DHS is verifying the work status on it. There are other documents the employer can ask for, as an example, a DHS I–9. They are running the SSN. They are getting a

verification back on it, and we are finding that that type of information is going to be much more current than anything you could embed on a card that is going to keep requiring people to come back to have their cards updated and information like that, which is a whole other workload, assuming that we could come up with a tamper-proof card.

Rick?

Mr. OUTLAND. Yes, Congressman, adding a photograph or a machine readable technology to the current card would obviously include changing the substrate from the banknote paper to a plastic substrate, say a polycarbonate or even a Teslin.

Now, while I have seen counterfeit documents produced on driver's licenses on Teslin and PVC, there are security features that are available that will make it more difficult for the counterfeiter to reproduce those. So, I agree with you. It can be done. You can produce a more difficult card. Given the document as it is right now on banknote paper, there are security features that can be added to that today at a nominal cost to also make it——

Chairman MCCRERY. Yes, a $10 bill, for example.

Mr. OUTLAND. Correct.

Chairman MCCRERY. We have just done it. I saw one the other day. It is very weird looking.

[Laughter.]

Chairman MCCRERY. I suppose it is better.

Mr. OUTLAND. Yes.

Chairman MCCRERY. Well, I want to give—you heard that. That is the House Democratic Cloakroom advising Republicans and Democrats we have votes.

[Laughter.]

Mr. LEVIN. You can stay if you want.

[Laughter.]

Chairman MCCRERY. I am going to yield. I have more questions, but I am going to yield to my good friend and colleague from Michigan, Mr. Levin, for any questions he might have.

Mr. LEVIN. Just a few, and then, I guess—maybe I will be very brief so Mr. Pomeroy can—the more I hear of this, in a sense the more confusing it is, though you are very articulate. It is not very—it is not clear to me what the issues really are. I take it there are numbers of citizens in the United States, of the United States, who do not have a SSN.

Mr. STRECKEWALD. There are—I am sorry, there are many, did you say? I could not quite hear you.

Mr. LEVIN. There are many.

Mr. STRECKEWALD. We do not believe there are too many people, citizens of the United States that do not have a Social Security card, because most parents get them right away for their newborn babies for tax purposes, and everybody else has one for work and for Social Security purposes.

Mr. LEVIN. Before that started, I take it there are some people here, citizens, who do not have a SSN, maybe older people, right?

Mr. STRECKEWALD. Well, most of our elderly, at one point or another, came into our offices to get benefits. Even those that did not work, there were some early provisions in Social Security for spouses' benefits if they did not work which still exist today. There

were some for Medicare. So, I believe that you would find that most elderly citizens——

Mr. LEVIN. Most.

Mr. STRECKEWALD. —have SSNs, if not all.

Mr. LEVIN. If we had an ID program, it would mean that there would be people who would not otherwise seek a SSN who would have to become participants in the program, right?

Mr. STRECKEWALD. Yes; I think what I hear you saying is, if we decided to issue a new card, there would be some people who normally would not be coming in to get a card, and we would not see them, because they are perfectly fine. Right now they do not need to show their card. They are retired or whatever. If they were asked to come in and get a new card, we would see a lot more people than we normally see for the general replacement card traffic.

Mr. LEVIN. Okay; secondly, if there were not an issue in this country about people who are working here, who are not here legally, would there be this issue of a national ID card? You are not sure.

Mr. STRECKEWALD. At Social Security, from that perspective, I am not sure. I would defer to the investigators and the experts at the table.

Mr. LEVIN. Well, maybe you do not want to answer that.

[Laughter.]

Mr. LEVIN. It is okay. The next thing that is rather confusing is that part of the problem seems to be that a lot of employers do not want to check the status, legal or illegal. Is that not true? Yes, it is true.

Mr. STRECKEWALD. I mean, in our experience, I think, the Inspector General's experience, that is definitely true.

Mr. LEVIN. So, if we have a card, it does not matter what you call it, it does not get at the issue of whether we are going to have an effective system of requirement when there is a larger issue as to whether or not people want to accurately and effectively check the status of people, right?

Mr. STRECKEWALD. For things to change from where they are now, there would probably have to be more enforcement on that part of the process; that they would have to check it and verify it.

Mr. LEVIN. Just to finish, let us say we had an ID card today, and we had a system that any employer who did not verify and use the system, punch into the computer would be guilty of a high misdemeanor, let us say, for example—I assume that would be a somewhat controversial proposition, would it not?

Mr. O'CARROLL. Yes, I would agree, because as it stands now, there are laws requiring employers to verify SSNs and provide valid numbers, and employers do not. There has not been very much enforcement done on that.

Mr. LEVIN. Thank you.

Chairman MCCRERY. Mr. Pomeroy.

Mr. POMEROY. Thank you, Mr. Chairman. I will be brief. Thank you for putting together this hearing, and the very interesting panel that majority staff selected has really done a nice job here of collecting a range of views on the proposal.

When I was in the State Legislature, now 25 years ago, we passed a law that the North Dakota driver's license number is the SSN. It was simple, easy, everyone remembers.

They changed that law. They really, upon further reflection, we really did not want Social Security kind of being a national ID, a national identifier; privacy today, privacy issues, identity theft issues, lots of things led the legislature to correctly, in my view, make that change.

I do think this issue presents in front of us very squarely, this would be moving the Social Security card to a national ID card. Now, whether or not that is the full intent of the proposal, I think that that is the effect of it. I have concerns about it in that respect, and I think that the panel has given voice to some of the reasons why one might want to think twice about that.

Another concern I have got is budgetary. This $9 billion cost of implementation is advanced at a time when the Administration has proposed changes in Social Security that would kick out of eligibility for survivors' benefits 16- and 17-year-olds. When my father died, I was 19, but I got benefits all the way through college. That was pre-1983. In 1983, we limited it to the 18th year.

I think depriving Social Security benefits to someone 16 is just wrong, absolutely wrong. If we cannot afford to pay 16-year-olds when they lose their Dad, I do not think we can afford $9 billion in these fancy cards; simple as that.

So, I have got some very deep reservations about this proposal. I thank the Chairman for letting me express them. I yield back.

Chairman MCCRERY. Thank you, Mr. Pomeroy. Gentlemen, we are going to have some other questions that we would like to submit to you in writing if that is okay, and that would allow you to leave when we recess in just a few minutes and not just hang around, because we are going to have votes until at least noon, it looks like.

However, I do want to point out to Mr. Pomeroy my observation that what some are proposing and what we are discussing here today is an enhanced SSN card, and then using that for purposes of employment verification or work authorization verification. I do not view that as a national ID card. I do not think it would be tantamount to a national ID card necessarily, because unlike, say, a driver's license, which we have to carry on our person if we drive or if we want to cash a check or whatever, one would not have to carry their Social Security card.

Only when he is applying for employment would he have to get it out of his safe in his house, or his drawer, or whatever, and take it down to that place of employment and say "here." Then, once that is done, he takes it back, and puts it back in his house in a safe place under his underwear or whatever.

[Laughter.]

Unless he is burglarized, his SSN is safe with him, just as safe as it is today, where the employer has to have it in any event; he does not have to see the card, but he has to have that number.

So, I think it is perhaps a bit of a jump to equate what we are talking about today with a national ID card and all of the ramifications of that. Would you disagree with my observations?

Mr. POMEROY. I think you make your point well, but my thought is in the end, if you need this identification card before you can get a job that we have taken a big step toward a national ID card concept, I think. I also do not know about, well, what other—unless we prohibit it in the legislation itself, what other groups may require the use of this particular card, because it would have—it would be the most advanced card in the marketplace, what other groups might require it for other purposes unless, again, we restrict it.

Chairman MCCRERY. Yes, well, that is a potential problem, but anyway, this is an interesting subject and an important subject, so I thank the witnesses very much for your testimony, and if you all have any thoughts on what I and Mr. Pomeroy just talked about, feel free to include those in your responses to written questions. Thank you very much. The hearing will be in recess until votes are concluded and we can muster the first panel.

[Recess.]

Chairman MCCRERY. The Committee will come to order. The hearing is adjourned.

[Whereupon, at 10:48 a.m., the hearing was adjourned.]

[Questions submitted by Chairman McCrery to the Honorable Jo Anne B. Barnhart and her responses follow:]

Question: If Congress were to require employers to verify an employee's name, SSN, and employment eligibility through a government database, would we still need to enhance the SSN card to prevent unauthorized work by non-citizens? Would some form of identification, (e.g., a driver's license or immigration card from the U.S. Department of Homeland Security) plus confirmation from the system be enough to identify individuals who do not have authorization to work in the United States? How much value would an enhanced SSN card add to such a system?

Answer: By using the Basic Pilot or a similar government database which accesses the Department of Homeland Security's (DHS) work authorization information, employers have access to the most current work authorization data available, because DHS' work authorization data is more current than the information on the Social Security number (SSN) card. Therefore, requiring employers to verify employees' work authorization through such a database, would render the SSN card, enhanced or not, of little additional value in proving current work authorization.

To address the issue of identity, employers would still need to verify an employee's identity by examining an identity document listed on the Form 1–9 and be alert for identity fraud situations. The Social Security card itself was never intended and does not serve as a personal identification document; that is, the card does not establish that the person presenting the card is actually the person whose name and SSN appear on the card.

Question: In his testimony, Mr. Streckewald said that replacing cards for 240 million cardholders nationwide would cost approximately $9.5 billion. How much would it cost if the agency issues new cards only to people in the workforce? What are your thoughts on allowing the SSA to charge a fee to offset some or all of those costs—what are the arguments for and against such an option?

Answer: Last year we estimated a card with enhanced security features, such as biometric identifiers, would cost approximately $25.00 per card. This estimate does not include the startup investments associated with the purchase of equipment needed to produce and issue such a card. Based on this information, our most recent 5-year estimate regarding the issuance of new enhanced cards to 170 million current workers and 5 million new workers annually is approximately $6.7 billion to replace the cards within 5 years and $7.4 billion to replace the cards within 2 years. This estimate includes all startup and ongoing costs.

More recent data, however, shows that the cost of issuing Social Security cards has increased by at least $3.00, due, in part, to new requirements for verification

of evidence. We will update our estimate when we have accumulated sufficient baseline data. In addition, when formulating an estimate based on a particular proposal, we would have to consider the details of the proposal, including the type of card enhancements required and the amount of time given to issue the enhanced card.

Finally, charging a fee for issuing these new Social Security cards, while ultimately a policy decision, would result in significant additional costs for the Social Security Administration (SSA). It would involve explaining and collecting the fee, obtaining credit card authorization if necessary, entering remittance of the payment into an automated system, and issuing a receipt of payment. In addition, charging a fee would involve SSA periodically setting a fee schedule and reconciling these offsetting collections. All of these actions would result in a considerable increase in the cost of issuing a Social Security card.

Question: What would be the effect on SSA's workloads of issuing enhanced SSN cards to everybody who is seeking employment in the United States? How many employees would it require to process the workload?

Answer: Issuing new enhanced cards to everyone seeking employment in the United States would have a significant impact on SSA's workloads until all individuals in the workforce have been issued a new card. We estimate that the initial workload would require about 13,000 additional employees. This equates to approximately 20 percent of SSA's current workforce. Absorbing this work without additional staff would require a reduction of 20 percent of the work we currently process, including retirement claims, disability claims and eligibility reviews. This estimate does not reflect the increased time our employees must spend with Social Security card applicants due to the new requirements for verification of documents which began in December 2005. We anticipate our workforce requirement would increase as a result of this recent change, but we need to develop a longitudinal baseline of actual data before revising our estimates.

Question: Another witness at the hearing, Dr. Kent, stated that "layering even the best current security on top of old data only gives the old data an appearance of being more trustworthy." Is the SSN system a good database upon which to build an employment authorization card? What changes, if any, would need to be made to the SSA's data to provide reliable validation of identity and employment authorization?

Answer: Social Security's databases do not contain current information about employment eligibility, because there is no SSA program need to maintain such information. SSA is able to verify current work authorization only when SSA records reflect that the individual is a U.S. citizen, because U.S. citizens have permanent work authorization. For all non-citizens, SSA's databases contain only a "snapshot in time" of employment eligibility as of the date the SSN card was issued. SSA's records are updated only when a non-citizen submits a new application requesting a change to the information in his or her record and provides evidence supporting the change. Therefore, DHS' work authorization data is the only reliable source for validating the current employment eligibility of non-citizens.

We believe an employment eligibility verification system, such as the current Basic Pilot, is the best tool for employers to verify employees' current work authorization status. Such a system uses the data contained in SSA and DHS databases in a way that allows each agency to maintain only the data necessary for the administration of their respective programs. As a result, each agency is able to focus on its own business processes, including the collection, integrity and accuracy of certain information. If these databases were to be combined, one agency would be burdened with the management of data which it does not collect, cannot verify and which is not related to its business purposes.

In addition, a combined database would be less accurate than two separate databases since combining the data would involve transmitting updated information from the source data base. At any point in time, some data on the combined database would be out of sync with the source database that contains the most current information.

Finally, we note that an essential component of any employment verification system is to confirm the identity of the individual seeking employment verification. SSA databases do not contain identity information and, thus, are not suited to this critical function.

Question: Currently the SSA issues a special series of SSNs to non-citizens who are assigned SSNs through the "enumeration-at-entry" program. If the SSA were to dedicate a special series of SSNs to individuals who have no authorization to work, or only temporary authorization to work,

at the time the SSN is issued, would that help employers identify non-citizens who are unauthorized to work in the United States?

Answer: SSA has considered using special series numbers for temporary non-citizen workers and those non-citizens admitted without work authorization. Our analysis showed that a special series for temporary workers would be of limited value in providing meaningful work authorization information to employers because immigration and authorization to work status may expire, be renewed or changed to another status by DHS. Thus, employers looking at a card or SSN with a special series designated for temporary workers would still need to verify current work authorization.

Other concerns to be considered with numbers that identify certain categories of non-citizens include the following:

- Providing new, special series SSNs for all aliens in the United States who have no work authorization or temporary work authorization, and who have already been issued an SSN, would present a staggering workload for SSA.
- SSA would also be required to assign new SSNs to non-citizens when their immigration status changes. The volume of new SSNs which would be required to assign multiple numbers to many non-citizens would create a number of issues, including:
  - Running out of numbers. (SSA currently has enough SSNs for nearly 70 years. Assigning multiple numbers to non-citizens would require setting aside large blocks of numbers, which would significantly deplete the supply of SSNs available to citizens.)
  - Complex cross-referencing of multiple numbers by SSA and all other governmental and non-governmental agencies that use the SSN.

Question: If Congress were to require the SSA to record information on when a temporary immigrant's authorization to work in the United States expired as part of its voluntary SSN verification services, would that help employers identify non-citizens who are unauthorized to work in the United States?

Answer: In keeping with DHS' mission and authority, DHS has the most current information on immigration and work authorization status. We believe that giving employers access to DHS' work authorization data, through an employment eligibility verification system such as the Basic Pilot, would be the most accurate way for an employer to determine an employee's current work authorization status.

While such information might be helpful to employers, requiring SSA to maintain such information would be problematic. Maintaining work authorization expiration information in SSA's records would expand SSA's mission to include a business purpose that would concurrently fall under the purview of DHS. Even if SSA were required to maintain such information in its records, SSA would not be responsible for granting work authorization status or determining the duration of such status. Therefore, SSA would be unable to respond to employer questions or to resolve issues related to the verification of that information.

[Questions submitted by Chairman McCrery to the Honorable Patrick P. O'Carroll and his responses follow:]

Question: Is there such a thing as a counterfeit proof card? How would you define a minimum threshold for a counterfeit and tamper "resistant" card?

Answer: We do not believe there is such a thing as a perfectly counterfeit-proof Social Security card. Certainly, with each new security feature, the card would be more tamper-resistant. However, we are uncertain as to whether trying to make the card more counterfeit-resistant is worth the costs of improving and reissuing such cards.

As a person ages, there are modifications in appearance such as weight gain or loss, changes in hair and facial appearance, and so on. Because of this, photographs often are not as reliable as other biometric alternatives. We believe that digitized fingerprints would be more reliable than photographs as scientific data suggests that a person's fingerprints do not substantially change after age 3. In addition, new photographs would need to be taken periodically to stay current with an individual's physiological changes. We also are concerned about the effect on SSA's Enumeration at Birth program of requiring such a card.

The Social Security Administration (SSA) will need sufficient time to design an enhanced card. It will need to determine which biometric features are to be captured, ensure proper data linkage with the Department of Homeland Security, and issue the new card to tens of millions of individuals. This will create a significant administrative and cost burden for SSA. A more viable alternative might be to issue

the new card only to new applicants, to those current number holders who apply for benefits in the future, and to those current number holders who request the new biometric card.

If the Social Security card is machine readable, then other public and private sector entities will need to procure equipment that can read the biometrics on the new cards. The costs to these entities, in terms of equipment and training, would need to be considered.

Question: There is much concern that non-citizens who are unauthorized to work are using counterfeit SSN cards and false or stolen SSNs in order to illegally gain employment in the United States. Is it the SSNs themselves, or SSN cards, that are most often used in connection with unauthorized employment?

Answer: Under current law, the SSN card is not a required document when an individual is applying for a job. If an applicant submits an SSN card to an employer, that employer may not identify a counterfeit card. Whether or not the employer views the actual SSN card, real-time verification with SSA of the name and SSN the applicant provides could assist in preventing theft of an individual's SSN or use of a false number. In addition, active deterrence, in the form of possible apprehension for false use of an SSN, would further decrease SSN misuse.

Although we do not capture this specific information about SSN misuse in our case management system, it has been the experience of our investigators that SSNs themselves, rather than Social Security cards, are most often used in connection with unauthorized employment.

Question: In your testimony, you said that your prior audit work has revealed inaccuracies in the SSA's SSN database that could affect the Agency's ability to provide employment eligibility verification services. Could you elaborate on what you found?

Answer: In our audit *Compliance with Policies and Procedures When Processing Noncitizen Social Security Number Applications at Foreign Service Posts* (A–08–04–14060, August 30, 2004), we found that SSA personnel classified 12 percent of the applicants enumerated at Foreign Service posts during our audit period as noncitizens, even though documents provided by the applicants showed them to be United States citizens. For these cases, the SSA employee recorded that United States citizens born abroad were noncitizens. We have additional audits that have identified similar issues. However, we have not performed a review of the overall accuracy of SSA's enumeration database. We do have a review ongoing in this area and will report the results when we have completed our review.

[Questions submitted by Chairman McCrery to the Dr. Peter Blair of the National Research Council and his responses follow:]

Question: Dr. Kent stated in his testimony that there are almost always forces that push identification systems to be used in ways for which they were not originally designed or intended. What do you think could be some of the unintended consequences of adding identity information, such as a photograph or other biometric information, to SSN cards?

Answer: The general issue of unintended consequences from the deployment of any large-scale identity system is described in the reports that Dr. Kent cited in his earlier testimony. Absent strong technical and policy countermeasures and disincentives, the use of an ID card, ID number, or ID system can expand greatly, just as has happened with the SSN and the state driver's license. Potential unplanned-for uses depend in part on the purpose of the system, what information is contained in any related databases, and what possession of an ID is meant to signify. Adding biometric information to the ID system implies another level of complexity with all of the attendant challenges surrounding enrollment, capture of biometric information, reliability, accuracy, and so on. To the extent that an ID system is made reliable and accurate, it is that much more tempting a target for attacks or simply for uses for which it was not designed. Predicting what specific secondary uses might arise for any particular ID system is difficult absent a more complete description of that system.

Question: If the role of the SSN card was expanded so that it provided proof of identity, would it become a more desirable target for identity thieves or others who seek to commit crimes using the SSN? Would the potential damage that could be done if an SSN is stolen by greater? How could we protect individuals, businesses, and the government against this?

Answer: To the extent that an expanded SSN card becomes more valuable—in this case "proof" of identity would be a valuable commodity—the more likely it is

to be a target for identity thieves as they seek to take advantage of the new functionality. Increasing the value of the SSN card might also raise its profile, even apart from any new credentialing that it could offer, and thus increase the frequency with which it is a target of traditional sorts of identity theft and fraud. Identity theft is already a major challenge by virtue of the link between the SSN and other readily available types of personal information and access to credit. Finding ways to cut these links so that identity credentials in one system cannot be easily used in another might offer some protection. On the other hand, this could insert friction and decrease efficiency of some transactions.

Question: What documents available today should employers use to verify the identity of their employees?

Answer: Our reports do not address this question specifically. To the extent that employers need to use an ad hoc or formalized identity system when hiring, questions that would help guide the choice of documents to use include: what specific problems need to be addressed (in this case, presumably, establishing work eligibility), what is the extent of the problem (affording some sense of costs and benefits), how could a particular identity system address that problem, and what other solutions (apart from a formalized new identity system) might address the problem?

Question: How would you define a national identification system? If Congress were to add certain features to the SSN card, such as a photo or other biometric information, and to require its use to obtain employment, do you think it would meet that definition?

Answer: Our reports do not draw a clear distinction because any large-scale identify system poses numerous challenges and policy questions that must be addressed. For some systems, such as those deployed only to allow access to a particular business building for example, the scope and scale is fairly limited and the policy issues are primarily specific to that business or that location. However, in any system that is deployed to encompass large portions of the population for more general purposes much more rigor and attention to the questions outlined in *IDs—Not That Easy* are needed. In this sense, then, there are already several nationwide identity systems, each serving different purposes, including passports, driver licenses, and present-day SSN cards/numbers. In short, changing the SSN card's features and functionality would create a national identification system much as the existing systems listed above have, but the label is much less important than is sorting through the policy and technical challenges of any large-scale identity system.

Question: Members of Congress have introduced proposals that would require millions of employers across the United States to access an employment eligibility verification database operated by the government. What concerns would you have about the privacy and security of such a database? What is the track record on maintaining the security of such a database?

Answer: Such a database would presumably be one element of a large-scale identity system and all of the issues raised in our two reports would apply. Securing the database is only part of the challenge. Depending on the purposes of the system and the specific content of the database, such a database could be an extremely high-value target for a wide variety of people ranging from tax avoiders to identity thieves to national security risks. Just as with a state driver's license system, the value of this database as a target will be dependent on what value the credential offers; the more things the credential is useful for, the higher value target the database is likely to be.

An early question to ask is how is membership in the database ascertained and verified? That is, what process determines whether an individual is eligible to work? Then, additional questions include: What individuals, organizations, and institutions would have legitimate access to the database? How would that access be facilitated? Who would verify the legitimacy of these individuals, organizations, and institutions? What opportunities for redress would there be if erroneous data ends up in the database? Where would liability for mistakes reside? All of these points, and many others, introduce various sorts of privacy and security vulnerabilities into the system. And, experience suggests that even applying the best security and privacy protections available will not protect against so-called "social engineering" attacks or hacks (such as bribes). That said, protection against attacks is only one part of the challenge. Having policies, procedures, and technical capabilities in place to discover that an attack has taken or is taking place as well as procedures in place to respond effectively is also critically important. Virtually any large, valuable database will be the target of some kind of attack and no such database can be 100% secure; therefore clearly thinking through how to respond in the event of an attack,

disclosure, or simple failure is a key component of building secure and reliable systems.

[Submissions for the record follow:]

Severn Trent Services
Colmar, Pennsylvania 18915
March 27, 2006

The Honorable Bill Thomas
Chairman
Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Thomas:

I am writing on behalf of our company in support of H.R. 1708, the Clean Water Investment and Infrastructure Security Act. Severn Trent Services has a global presence and is a $600 million business employing 2,350 personnel providing water and wastewater equipment and services to communities and industrial customers around the world. The company's broad range of products and services is concentrated around disinfection, instrumentation, and filtration technologies, pipeline analysis, rehabilitation and repair services, contract operating services and state-of-the-art residential metering products and services. Severn Trent Services is a member of the Severn Trent Plc (London: SVT.L) group of companies. An international environmental services leader, Severn Trent is a FTSE 100 company.

We should all be concerned about the deteriorating state of our nation's water and wastewater infrastructure. Nearly $1 trillion dollars need to be invested over the next 20 years to repair, rehabilitate, replace and upgrade our nation's network of water and wastewater treatment plants, collection systems and distribution lines. Failure to stem this looming crisis will cause significant public health and economic harm to our country.

H.R. 1708 will allow communities across the nation to partner with the private sector in funding critical water infrastructure activities by removing water and wastewater projects from the state volume caps for private activity bonds. This is the least expensive option for addressing a growing national crisis and ensuring that all Americans are guaranteed a safe, reliable water infrastructure system. We urge Congress to move expeditiously on this proposal and thank you for your leadership in this matter.

Sincerely,

Steve Hinkle
Credit Manager
Michael P. Isabell
Business Unit Manager
Linda D. Slack
Administative Assistant
Nadia Abbott
Marketing Manager
Barbara Ferns
Principal Electrochlorination Engineer

○